2010

Data privacy: Legal and business malpractice

Gulmira Zhavgasheva

Data Privacy: Legal and Business Malpractice

By

Gulmira Zhavgasheva

Thesis submitted in partial fulfillment of the requirements for the
degree of Master of Science in
Networking and System Administration

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

November, 2010

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

Master of Science in
Networking and System Administration

Thesis Approval Form

Student Name: Gulmira Zhavgasheva

Thesis Title: Data Privacy: Legal and Business Malpractice

Thesis Committee

Name	Signature	Date

Charles Border, Ph.D.
Chair

Luther Troell, Ph.D.
Committee Member

Sumita Mishra, Ph.D.
Committee Member

Thesis Reproduction Permission Form

Rochester Institute of Technology

B. Thomas Golisano College
of
Computing and Information Sciences

Master of Science in
Networking and System Administration

Data Privacy: Legal and Business Malpractice

I, Gulmira Zhavgasheva, hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: _____ Signature of Author: _____

Abstract

While banking system of Kazakhstan has been reformed during the past two decades to transition to the international standards, privacy of financial information seems to be left neglected. With the advent of the technological era and, hence, the rapid growth of computer crime, privacy of financial information has become a primary necessity in the context of relationship between financial institutions and their customers. However, collecting, storing, processing and transferring such data raises issues regarding security and privacy of customer's data. The purpose of this research was to evaluate the extent, to which privacy of credit card and cardholder data was considered and implemented in the banking sector of Kazakhstan. The research also sought to explore perceptions of banks (as in bank employees) in terms of data privacy awareness and their understanding of its significant importance, as well as concerns of bank customers in terms of privacy of their banking information. This data was collected through the qualitative analysis of 23 participant interviews. The participants came from three areas, which built the context of the research– legal, banking sector and its customers. The findings of the study demonstrated that data privacy was not paramount in the bank-customer relationship. It was explained by the lack of regulatory approaches in the sphere of data privacy within government and industry levels. Consequently, financial institutions lacked data privacy awareness. The findings also suggested that a knowledge gap in terms of data privacy existed between banks and their customers, whose level of privacy concerns was driven either by trust or indifference. This paper proposes constructive suggestions for the banks on how to better address the current issues of data privacy and associated requirements.

This thesis is dedicated in loving memory of my grandfather,

Zhashibek Dospol-uly,

who wanted to see me achieving this goal.

Acknowledgements

I would like to express a gratitude to my advisor and chair, Prof. Charles Border, who has mentored and supported me with enormous patience, especially at the times when I wandered away.

I must thank those, who participated in the research interviews. Particular thanks go to Nurlan Uspanov, conversations with whom helped me better understand the current trends in the bank's data privacy practices.

Finally, I would like to thank my family and Conzetti Finocchiaro for their love, support and inspiration. My sister, Botagoz, deserves special thanks, for her understanding and encouragement when I needed it the most while studying on the other side of the world. Most of the interview participants were recruited with her help. She also assisted me with the transcription of the interviews. This work would not have been possible without her incredible assistance and endless faith in me.

Contents

List of Figures

1. INTRODUCTION

Information is recognized to be a fundamental and most valued asset of any organization. Hence, data collecting, processing, storing and revealing to external parties requires more and more guarantees over its privacy. This is especially true when dealing with personal information and financial information in particular, which have become more accessible with the rapid development of computer technology and computer crime.

In this regard, the U.S. National Institute of Standards and Technology (NIST) uses a term "*personal identifiable information (PII)*" as personal information, and defines it as "*any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information"* (McCallister, Grance, & Scarfone, 2010).

The European Union Data Protection Directive (Directive 95/46/EC), whom regulates the processing of personal data within the EU, has a similar term – "*personal data*" that "*shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" ("On the Protection," 1995, p.12).*

The Government regulation of the Republic of Kazakhstan, “On approving of the list of personal data of individuals included in the government electronic information resources,” defines the list of personal data for an individual as *“last name, first name, middle name; date and place of birth; nationality; gender; marital status; citizenship; unique identification number; photograph; address; passport data”* (The Government Regulation, 2007)

Laws and regulations on data privacy, as well as definitions of personal information, are unique for each state (country) or organization. However, they all share the common goal of protecting personal information. Compromised personal information creates a risk for identity fraud and/or identity theft, which may cost organization millions of dollars along with the loss of public trust and business reputation. Regulations on processing, movement and protection of personal data are being developed worldwide, but the requirements are not entirely considered nor implemented in some organizations. The research performed was done in an effort to examine Kazakhstan’s banking sector, as the state of information security and data privacy was found to be dismal. This research attempted to investigate current perceptions and concerns of banks and its client-base related to the issues of privacy of credit card and cardholder data. No previous studies to examine this problem in the financial sector of Kazakhstan were discovered.

2. BACKGROUND AND RATIONALE

2.1 Historical Overview

The contemporary banking system of Kazakhstan was developed in stages, being initially formed from within a single credit-banking system of the USSR (The Government Regulation, 2007; General Information About, n.d.). Reforming of the existing banking system of the Kazakh Soviet Socialist Republic (SSR) had started in 1987, when it was decided to create a two-tier banking system in the USSR. However, this process was interrupted in the late 1980s, when the significant political events had influenced the Soviet Union, and further followed by its liquidation and establishment of the Commonwealth of Independent States (CIS) in its place, which made all the fifteen republics of the USSR independent and sovereign. Thus, with the final dissolution of the Soviet Union, the Kazakh SSR was renamed the Republic of Kazakhstan, and declared of its independence on December 16, 1991 (Lyakhov, 2002).

The next phase of the banking reform started with the National Bank's new role as the republic's central bank, representing the first tier of the existing banking system. The second-tier was composed by the rest of the banks, except for the Development Bank of Kazakhstan due to its special legal status (General Information About). With the given power, the National Bank of Kazakhstan (NBK) was authorized to represent the country's interests "in the relations with the central banks, with banks of other countries, in the international banks and other financial-credit organizations" (General Information About). At the same time, a number of commercial banks rapidly rose due to introduction of the national currency – Tenge. In 1993, two new laws titled "The National

Bank of the Republic of Kazakhstan" and "About banks and banking activities in the Republic of Kazakhstan," which founded a legislative base for reforming the old banking system and creating the first commercial and private banks in Kazakhstan were adopted; throughout time, they have been revised and updated to appropriately reflect new requirements of the changing environment (The Law of the Republic of Kazakhstan No. 2155, 1995, The Law of the Republic No. 244, 1993/1995).

A banking reformation continued with the diminution of the commercial banks in the country, which largely occurred due to non-compliance with the NBK's strengthened regulations for the second-tier banks, as well as increased competition between them. Additionally, the NBK and Financial Markets Supervisory Agency of the Republic of Kazakhstan (FMSA) have gotten an authority to inspect commercial banks on a regular basis, and consequently, the banks were also required to periodically report to them. Thus, the NBK's supervisory functions and regulatory actions greatly raised reliability of the banking system (Kasera, 2007; Report and Recommendation, 2005).

Overall, the country's transition to a market economy has significantly changed its financial institutions and related legislation, bringing along development challenges and reforms. It also assisted Kazakhstan's banking sector to implement "prudential standards, including requirements on capital adequacy, liquidity ratios, transparency as to the auditing of banks by local and international auditors, synchronization of local accounting practices with International Financial Reporting Standards (IFRS), and personnel training programs" (Report and Recommendation). All this should have allowed commercial banks to attract foreign investors.

Transition of commercial banks to the international standards was defined in the NBK's regulations, which required banks to become compliant by January 1st, 2001 (The National Bank No. 292, 1996; The National Bank No. 32, 2001). These regulations aimed to adopt international banking best practices in order to strengthen and increase financial stability of the banks. According to these regulations, all banks of Kazakhstan should have met requirements of the international prudential standards (mentioned above), including those regarding customers' data protection and data communication.

The main objective of deploying standards and regulations for the protection of data privacy in banks is to minimize risks of compromising customer data. Not only does this require adequate privacy regulations that will give employees and customers tools to help them recognize privacy vulnerabilities and threats in place, but also mandates compliance with such regulations in order to constantly retain the confidentiality and integrity of sensitive information. If there are no such standards or regulations, banks must create and implement their own strategies and practices, which would ensure privacy and security of cardholder data. However, achieving data privacy compliance might become a challenging task for any organization, when it is lacking of the appropriate theoretical knowledge, practical experience and computer technologies in the sphere of information security. This task becomes even more challenging for Kazakhstan's banking system, which was rebuilt from an old system, proved inefficient, and is still in its development process on the second decade of the country's independence.

2.2 Significance and Purpose of the Study

This research focused on legal framework and practices on privacy of cardholder information in Kazakhstan's banking sector that claims to be following the Payment Card Industry Data Security Standard or PCI DSS, as the banks partner with the card brands that collaboratively developed this security standard of the USA. Contrary to this claim, privacy issues were found and personally experienced by the researcher, who has been a customer of one of the banks in Kazakhstan, monthly receiving bank-statements via e-mail (Fig.1). Received bank-statements also contained cardholder's payment card number, name and social security number. Needless to say that having all this data in the statement makes cardholder information unprotected, hence, easier to become compromised and be used in a fraudulent transaction. According to PCI DSS, "if cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN [Primary Account Number], or are otherwise present in the cardholder data environment, they must be protected in accordance with all PCI DSS requirements except Requirements 3.3 and 3.4, which apply only to PAN" ("Requirements and Security," 2010). Thus, the researcher made an assumption that the importance of privacy and security of the cardholder data has been underestimated, not completely understood or considered in the bank's data privacy practices.

This research sought to evaluate understudied issues of privacy regulations in Kazakhstan banks, as well as analyze how these issues could impact customers (cardholders) and the way banks do their business. It will help banks better understand the importance of data privacy and cope with the issues they currently experience. It will also draw their attention to a need for a better relationship with cardholders, to be built

on trust and cooperation, always tending to work better in safeguarding cardholders' data. The research questions addressed by this study are given in the next paragraph.

Cardholder Contract Statement

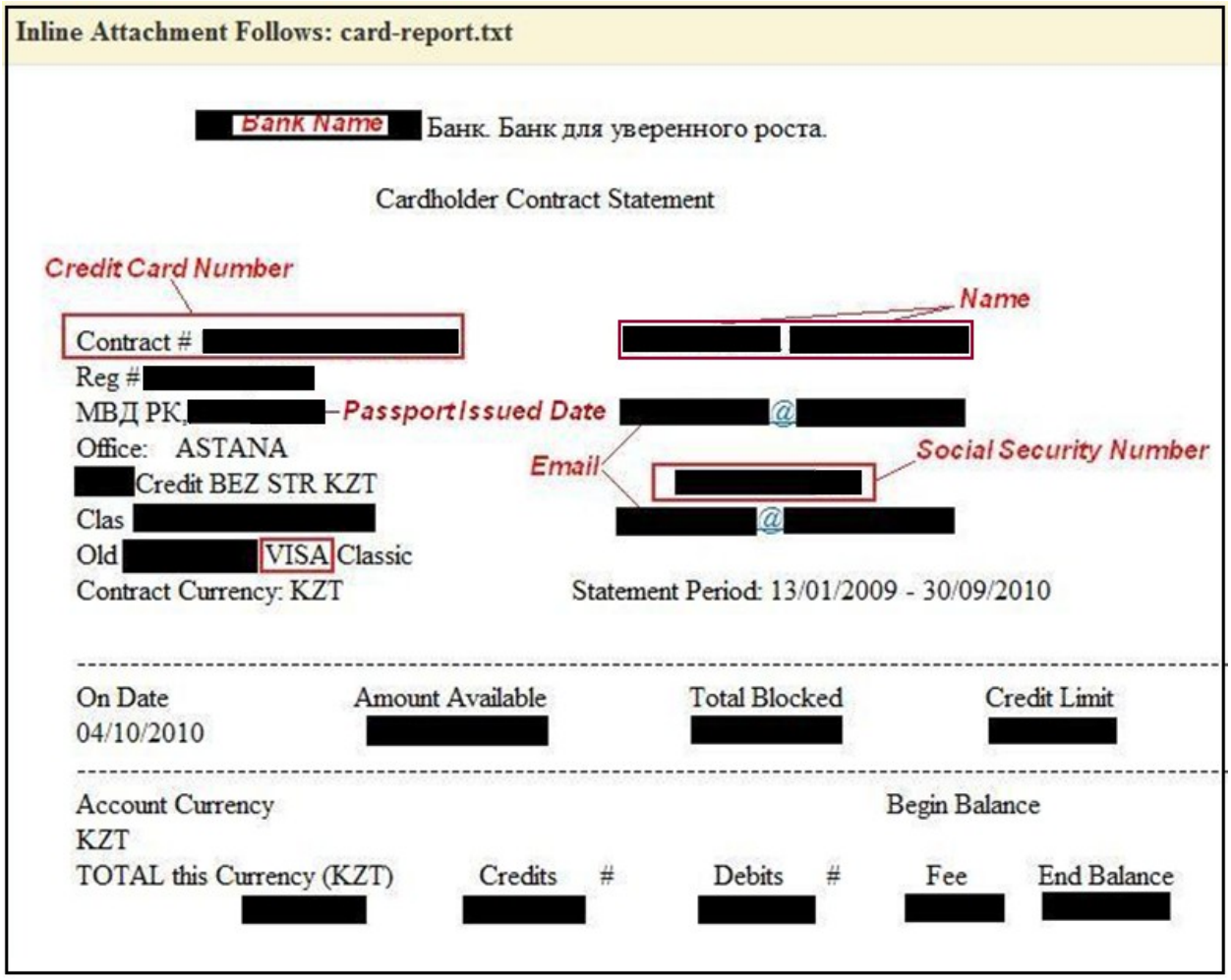

Figure 1: Individual's card-statement, monthly received via e-mail.

2.3 Research Questions

The following questions have led the study:

1. To what extent, if any, is privacy of credit card and cardholder data considered and implemented in the banks of Kazakhstan?

2. What is the banks' level of data privacy awareness? How well do they understand the importance of data privacy?
3. To what extent, if any, are the bank customers concerned about privacy of their credit card and cardholder data?

2.4 Definition of Terms

Definitions of the key terms used in this research are presented in this section:

Authorization: "Granting of access or other rights to a user, program, or process. For a network, authorization defines what an individual or program can do after successful authentication. For the purposes of a payment card transaction authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor" ("Requirements and Security," 2010).

Cardholder: "Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card" ("Requirements and Security," 2010).

Cardholder data: "At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction" ("Requirements and Security," 2010).

Compliance: Organization's conformity with predefined standards, regulations or laws on certain subject.

Compromise: “Also referred to as “data compromise,” or “data breach.” Intrusion into a computer system, where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected” ("Requirements and Security," 2010).

Credit card fraud: A theft of someone’s credit card information for getting access to their bank accounts for own benefit.

Identity theft: Also referred to as “identity fraud,” or “impersonation.” A theft of someone’s personal information in order to personate a victim or victims, typically, to access their resources for own benefit.

PAN (Primary Account Number): Also referred to as “account number.” It is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account ("Requirements and Security," 2010).

Participants: People, who were selected from three fields of interest to be interviewed for this research study.

Personal information: Also referred to as “personally identifiable information (PII),” or “personal data.” “Information that can be utilized to identify an individual including but not limited to name, address, social security number, phone number, etc.” This term is usually determined by state laws or regulations ("Requirements and Security," 2010).

Policy: “Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures” ("Requirements and Security," 2010).

Privacy regulations: State rules relating to a collection, use, retention, disclosure and protection of personal information by entities, whose services are used by individuals for different purposes.

Transaction Data: "Data related to electronic payment card transaction" ("Requirements and Security," 2010).

2.5 Delimitations

1. The participants of this research study were delimited to the sampling from the legal department (lawyers, in particular), bank (employees from Credit Card departments, in particular) fields and bank customers (cardholders, in particular).
2. The data source was delimited to the general legal framework, available on the official sites of the Ministry of Justice of the Republic of Kazakhstan and National Bank of the Republic of Kazakhstan.
3. The research study was delimited to the data provided by the participants during the interviews.

2.6 Limitations

1. The research results were limited to the accuracy of the information provided by participants.
2. The research results were limited to the validity and reliability of the methodology approach, chosen for this study.

2.7 Organization of the Study

Chapter 1 presented introduction to the research. Chapter 2 introduced historical background and rationale for this study. Chapter 3 will offer a review of the current and

relevant literature to establish the context for the research problem. Chapter 4 will present a design of research describing the methodology of data collection and analysis. Chapter 5 will present the research findings with their analysis and interpretations to address three research questions of this study previously detailed in Chapter 2. Chapter 6 will present a conclusion of this study, recommendations and scope for future research. Appendices will present data source collected from the interviews with three groups of participants.

3. LITERATURE REVIEW

3.1 Overview

To understand an importance of protecting credit card and cardholder data, consider first an increasing number of credit card fraud both online and offline. Different aspects of data privacy concerns range from the demand for compliance with the state (countries) laws and regulations (McCallister, Grance, & Scarfone, 2010; "On the Protection," 1995; "Requirements and Security," 2010) to the analysis of the factors that determine those concerns (The National Bank No. 325, 1999; The National Bank No. 400, 2000) are given in the current literature review.

The first portion of the related literature work gives an overview of the existing legislation in Kazakhstan that is somewhat relevant to the privacy of personal data. Then, a number of guidelines, created (worldwide) to help organizations with protecting confidentiality of personal data they collect, use and transmit, are introduced for a reader's insight. The examination of consumer trust and their privacy concerns will be introduced next. And the summary of the current and relevant literature around this research study will finalize this chapter.

3.2 Legislation Framework

The necessity to build effective paths for Kazakhstan's economic and financial activities arouse from the country's sovereignty declaration and its transition to a market economy. In February, 1995, the Program on Banking System Reform with determined

priorities such as transition to the market economy and creation of proper financial markets was adopted in Kazakhstan.

In that same year, with regard to the banking system, the laws “About banks and banking activities in the Republic of Kazakhstan” and “About the National Bank of Kazakhstan” were ratified (The Law of the Republic No. 244, 1993/1995; The Law of the Republic of Kazakhstan No. 2155, 1995). These two laws marked the beginning of Kazakhstan’s banking system reforms and defined main goals, functions, activities, legal status and powers of the National Bank of Kazakhstan, regulating its role in the banking system and its relationships with other state agencies and foreign countries.

Even though, reforms in the legislation have improved the banking system and its regulatory framework, they didn’t seem to develop privacy laws or regulations in the sphere of financial data. The analysis of the country’s current legislation showed that none of the existing laws or policies solely and explicitly regulates privacy of personal information or, credit card and cardholder data, in particular. There are some laws and regulations that touch on this aspect poorly (The Law of the Republic No. 474, 2003; The Law of the Republic No. 237-I, 1998; The Law of the Republic No. 370-II, 2003; The National Bank No. 179, 2000; The National Bank No. 146, 2000; The National Bank No. 325, 1999; The National Bank No. 400, 2000; The National Bank No. 242, 1998; The National Bank No. 386, 1999).

The Government regulation (2007) defines what data is categorized as personal, but it does not include banking information as part of it.

The Civil Code of the Republic of Kazakhstan dated 27 December, 1994 (No. 23-24), includes protection of the rights of entrepreneurs and consumers, as well as their trade secrets. In addition, it also states that every consumer has the right for “complete and accurate information about goods (work, services)” (The Civil Code, Article 10, sub-paragraphs 5, 6).

The Civil Code also includes the basis for personal privacy (Article 115, sub-paragraph 3), and protection of the confidential information that “constitutes proprietary or trade secret” from being exposed to third parties. The damage caused by its illegal revealing must be compensated by an employee who exposed it and a person who obtained it without authorization (Article 126). And finally, Article 144, sub-paragraph 1, states that a “citizen has the right to protection of [his] bank secrecy” (The Civil Code).

To ensure the price stability in the Republic of Kazakhstan, the NBK carried out the following functions: “development and implementation of the monetary policy of the state; support of the payment system functioning; implementation of the currency regulation and currency control; assistance in support of stability of the financial system” (Report and Recommendation, 2005; Payments and Securities, 2006). The Law of the Republic of Kazakhstan No. 244 also restates a basic function of the NBK as “the maintenance of the functioning of the payment systems” (Article 7, sub-paragraph 2, 1993/1995). In addition, the basis for the payment system oversight function is stated in Articles 8 and 48. In 2005, several modifications were made, where the NBK’s oversight function and main responsibilities were clarified. Paragraph 2 of the latter article stipulates the following: “… to oversee the payment system NBK has a right: to issue regulations, defining the conditions and organizational procedures for the functioning of

the payments system; to monitor and assess the organization and functioning of the payment system; to obtain information from participants and payment system operators; to perform surveys of payment system participants' according to the legislation and NBK regulations… "

Articles 49 and 52 allow the NBK to open accounts to commercial banks and non-bank organizations (The Law of the Republic of Kazakhstan No. 2155, 1995).

The Law of the Republic of Kazakhstan No. 244 contains the legal underpinning for opening banks, branches, their diminution and licensing, and also defines banking regulations, prudential rules and obligatory norms and limits (1993/1995). Article 33 states a contract based relations between bank and its customers. Article 44 provides the rights for audits and inspections of banks by the FMSA, as well as NBK. On the other hand, this law has no explicit statement about the privacy of credit card and cardholder data, nor does the law on the NBK (The Law of the Republic of Kazakhstan No. 2155, 1995).

3.3 Security Governance – International Approach

As credit cards have gained greater purchasing power in domestic and foreign locations, making it possible to use them worldwide, it has also brought up serious challenges with maintaining their security. With the peak of Internet purchases and online transactions, it is now enough for criminals to obtain credit card numbers rather than cards themselves, to carry out their fraudulent activities. The threats to the security of credit card made some countries enact special legislation and strict punishments for apprehended violators. However, credit card fraud has no geographical boundaries;

fraudsters continue to improve their scenarios and go internationally. This made some countries collaborate to reduce such losses by sharing technologies, standards, regulations and experience between their financial institutions and governmental agencies. This cross-border partnership has already shown a promise, but it still needs to improve because cybercrime imposes greater challenges. Thus, governments should foster improved communication and collaboration between each others' legal, financial and information technology sectors to fight domestic and international credit card fraud.

Today, numerous international privacy guidelines exist in the world. One of them requires a special attention – the U.S. Payment Card Industry Data Security Standard (PCI DSS); any organization that stores, processes and/or transmits payment cardholder information associated with American Express, Discovery Financial Services, JCB International, MasterCard Worldwide, or Visa Inc. International must comply with this standard that was specifically designed to help organizations in protection of credit card and cardholder data ("Requirements and Security," 2010).

PCI DSS is a set of requirements, which represent minimum technical and operational measures designed to ensure security of credit card and cardholder data. It was collaboratively developed by the mentioned above main payment card organizations, who jointly found the PCI Security Standards Council. A factor that defines applicability of these requirements is PAN ("Requirements and Security").

The standard is comprised of six principles and twelve requirements, which demand implementation of policies or technology solutions to be compliant ("Requirements and Security"):

- Build and Maintain a Secure Network:

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

- Protect Cardholder Data:

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

- Maintain a Vulnerability Management Program:

Requirement 5: Use and regularly update antivirus software.

Requirement 6: Develop and maintain secure systems and applications.

- Implement Strong Access Control Measures:

Requirement 7: Restrict access to cardholder data to business need-to-know.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical access to cardholder data.

- Regularly Monitor and Test Networks:

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Regularly test security systems and processes.

- Maintain an Information Security Policy:

Requirement 12: Maintain a policy that addresses information security.

A use of technology solutions is not demanded for implementing of Requirements 9 and 12 in an organization. Requirement 9 only instructs how organizations should address restricted access to the locations where they store or process cardholder data. Requirement 12 dictates that organizations must maintain information security policies,

to which their employees, contractors, and everyone else in the organization that works with cardholder data must be introduced to and made to strictly adhere to.

Another, reasonably sufficient privacy guidance that drew researcher's attention is European Parliament and Council Directive 95/46/EC of 24 October, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, also referred to as Directive 95/46/EC ("On the Protection").

Directive 95/46/EC has become an important part of the EU privacy and human rights law regulating the processing of personal data with regard to its free movement within European borders. This regulation applies to data regardless of whether it is electronic or filed on paper. Directive was established by the European Commission and is addressed to all EU member states that must transpose the regulation into internal law. In addition to it, the member states should also have independent legislation on data privacy, being required to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" ("On the Protection," pp. 6, 12)

Directive determines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" ("On the Protection," p. 12). According to this broad definition, personal data can also be an individual's SSN, payment card number or any health information, thus making Directive applicable to financial or medicine sectors of the EU.

It is also important to note that data processing, according to Directive, is “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction” ("On the Protection," p. 12).

The Following highlights some of the guidelines of Directive 95/46/EC (“On the Protection):

- “Personal data must be processed fairly and lawfully; collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; adequate, relevant… accurate and kept up to date” (p. 13).

- “Personal data may be processed only if the data subject has unambiguously given his consent” (p. 14).

- “Member States shall guarantee every data right to obtain from the controller without constraint at reasonable intervals and without excessive delay or expense” (p. 17).

- “Member States …must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to

the risks represented by the processing and the nature of the data to be protected" (p. 20).

- "Member States shall adopt suitable measures to ensure the full implementation of the' provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive" (p. 23).

3.4 Trust and Privacy Concerns

It is clear that trust is fundamental for privacy concerns, thus it should be taken into consideration when creating privacy statements and safeguards, in order to establish strong and long lasting relations with consumers. Tsarenko and Tojib (2009) examined the driving factors of consumer privacy concerns in the financial sector, and tried to develop a customer typology based on customers' attitude towards privacy of their data. The authors picked this sector for the research as it "is known to be highly sensitive with customer privacy concerns" (p. 469). The authors' research indicated that "the level of privacy concern is primarily driven by trust that far outweighs any concerns with privacy statements and the provision of nationally legislated safeguards" (p. 473). Furthermore, they analyzed a customer cluster of financial services and it helped to reveal three different customer segments in the area: the pragmatist, indifferent, and competent. The research focused on segmenting customers based on their concerns about data privacy. The customer typology was built off of three determinants, which were trust based: willingness to provide information for compensation, concern with privacy legislation, and concern with privacy statements. "The growing importance of technology has made trust and privacy increasingly important. Such issues are

fundamental to attempts by financial institutions to build meaningful and lasting relations with their client base" (p. 475). Their findings indicated that trust was the biggest factor of privacy concerns, even though privacy legislation was confirmed as an antecedent, along with willingness to reveal private data in exchange for compensation. At the same time, age and education appeared to be significant variables in the identified segmentation: the lower level of education, the lower concerns about privacy along with moderate or neutral attitude towards trust, legislation and willingness to disclose own information for reward. Those that had some form of a higher education possessed a greater concern about the privacy of personal data, the legislation for privacy, and also had significantly lower trust.

An overall recommendation of this study was to urge financial organizations to focus on building trust with their "client base", helping them to reduce their privacy concerns and better inform them about employed privacy regulations and statements.

This research is a significant resource for the current study as it gives an empirically validated classification of customers based on their privacy concerns, which is applicable to all consumers of any country, and helps to better understand the privacy phenomena in the financial sector of Kazakhstan. It also makes it clear that financial institutions need to work towards their clients' privacy concerns more seriously, as this will further help both parties to build a trustworthy relationship.

Wang reported on the privacy issues related to the Internet marketing activities (Wang, Lee, & Wang, 1998). Being published back in 1998, the study's taxonomy of individual online privacy concerns, such as improper acquisition, improper use, privacy invasion

and improper storage of personal information is still applicable to the Internet marketing of today. Improper acquisition defined unauthorized access to a consumers' private computer in order to (improperly) collect his/her personal information and (improperly) monitor their online activities, which usually lead to improper analysis of the received data. Concerns about improper use were related to unauthorized analysis of consumers' personal information per their shopping and spending preferences and behaviors, which also could result in its improper transfer (Wang, Lee, & Wang, 1998). Concerns about privacy invasion referred to spam as a transmission of unwanted information to potential Internet consumers without their prior consent. And improper storage related to concerns about confidentiality and integrity of personal information.

Wang pointed that the key issue of privacy in the Internet marketplace was to balance the privacy rights of individuals with the benefits that the free flow of information provided. Here, I cannot agree with this point. Privacy rights of individuals are the safeguards they have to maintain confidentiality over their personal information. Personal information of individuals should be protected from "free flow", especially when it is going to be used to benefit some interested parties. Thus, privacy rights of individuals cannot be "balanced" with such benefits.

Wang suggested that privacy protection should have been undertaken in combination with three main parties involved:

Government – to promote privacy legislation and establish commissions to audit organizations' compliance with it; to educate the public about privacy issues; to encourage organizations' self-regulation (p. 66).

Businesses – to promote "self-regulation for fair information practices" (p. 66).

Individuals – to adopt “privacy enhancing technologies, such as network and information security tools” (p. 66).

I believe Wang’s last two party roles were not fully defined. Creation of one’s own privacy practices is not enough, in addition to it, businesses have to make sure they are implemented and strictly followed within the organization itself. It is also important to include employee awareness programs and education of their client base, when promoting any security practices. Having an internal auditing for proper implementation of privacy would also enhance this role.

The role of individuals is not nearly close to the reality. The assumption that an average individual would not be an advanced user of computer and IT technologies should come in at first place. Therefore, this role fails immediately. Individuals must first get familiar with the basis of information privacy and the issues it raises. This includes their privacy rights and existing legislation in the state and organization(s) they have to deal with, as in sharing their personal information.

Privacy of personal information is the ability of individual to seclude their information from public. But when this information is shared with commercial or government entities, chances that it would get disclosed or revealed without individual’s knowledge or consent are rapidly growing. Only a combined effort of government and financial industry can help to address privacy issues and enhance security of personal information.

3.5 Conclusion

Why are data privacy regulations required? Why should an institution comply with them? Dealing with sensitive information of any kind requires all systems of an institution to be secure and trustworthy. The odds of a data breach resulting in unauthorized access and information disclosure can be nearly eliminated by following specific data privacy guidelines. Having data privacy standards in place and complying with them means that the systems of institution are well safeguarded. In contrast, remaining non-compliant would most likely lead to a financial catastrophe, loss of business reputation and customers' trust.

The review of the national legislation provides a great insight into existing laws and regulations currently enacted in Kazakhstan. This also clearly demonstrates the absence of a proper data privacy legal framework, while other countries have successfully addressed this situation. Examining principles of international privacy standards and regulations can greatly contribute to the legislation of Kazakhstan, helping to create own regulatory approach for addressing data privacy concerns. This will also assist local financial institutions to build stronger relationships with their customers, whose trust is a major driving factor for credit card and cardholder data privacy concerns.

4. METHODOLOGY AND DATA ANALYSIS

4.1 Research Design

This research was conducted using a qualitative approach (Creswell, 1994/2003). The researcher has observed the topic and collected data by interviewing a multiple participants, which composed three aspects of the researched topic – the state's legal and financial sectors, and consumers of financial services, i.e. banks' customers. Participants were asked open-ended questions, in order to get in-depth information about their experience with the researched topic. The goal of this study was to explore and better understand what level of data privacy, if any, existed in the banking sector of Kazakhstan, and also to identify its perceived and actual value for the same segment. The study also sought to explore how the banks dealt with data privacy regulations, and what perceptions and concerns about privacy of banking information their customers had.

4.2 Purpose

This study aimed to: 1) determine, whether or not privacy of credit card and cardholder data was considered and implemented in Kazakhstan's banking sector, and what its current level is; 2) identify the data privacy awareness level and its importance as viewed by the banks, i.e. bank employees; 3) determine, whether or not bank customers were concerned about privacy of their credit card and cardholder data.

4.3 Sample Population

Initial observation of the research topic had identified three focus groups of participants to be interviewed: lawyers, bank employees – who worked in the administrative bodies and commercial banks, all operating in Kazakhstan, and bank customers – consumers of Kazakhstan banks' services. Each group, of varying numbers of participants (9 lawyers, 8 bank employees, and 6 customers), was subject to different questions, depending upon the field that participants belonged to. Interview results were analyzed and interpreted leading to the conclusions and recommendations of this research.

The lawyers needed to be interviewed to get to know what legislation per data privacy, if any, existed in Kazakhstan; what aspects it did or did not cover; and how it impacted banking sector, in particular. Interviews with the bank employees were supposed to give more insight of how banks handled privacy of cardholder data, whether they implemented PCI DSS or not; how keenly they were aware about data privacy and their current issues with it, as well as how important it was to them. Responses from the bank customers were supposed to identify, whether they were concerned about privacy of their banking information or not; what level of data privacy awareness they had – what they thought and knew about it.

4.4 Interviews Development

The observation of the current and relevant literature around the problem of this study and the researcher's own experience helped to develop the interviews for each identified group of participants that presented three aspects of the research study. The interviews collected data on: existing legislation per security and privacy of banking information in Kazakhstan; bank employees and cardholders' awareness of data

(banking information) privacy; bank employees' perceptions of its importance and cardholders' concerns about privacy of their information. The interviews' format included only open-ended questions, which assumed to get more insightful information from the participants. Each group of participants had a different set of questions; questions within one group have been slightly varied, depending upon respondent's experience with the essence of the researched problem, which was the driving factor of each interview.

4.5 Data Collection

All data source for the research was collected through the on-phone interviews with the individuals that were identified as belonging to one of the three focus groups of this study. The interviews were transcribed while they were taken. Insurance of the interview's confidentiality was provided in a form of informed consent that was sent to the participants via e-mail (Appendix A). All participants were subject to different set of questions, which, in turn, could have varied, being of a qualitative nature that assumes to have open-ended questions with their own variations, dependent upon the participant's experience, knowledge and willingness to provide more information.

4.6 Data Validity

The interviews were developed based on the researcher's empirical knowledge combined with the theory gathered from the literature review. The primarily basis of the research questions was the researcher's own experience. The interview questions used the key characteristics that were found in the existing literature. Similarity of the answers given by different participants from the same focus group ensured a validity of the collected data.

4.7 Methodology Limitations

This research study was qualitative descriptive, which is why the findings are not be applicable to other state sectors or organizations as the research was not projected to a wider audience, nor meant to provide a statistical analysis of any kind. The sample population was restricted to three focus groups that were relatively small, but had key characteristics in common. The objectivity of participants' responses determined accuracy of the held interviews, and there was a possibility that they were reluctant to answer some interview questions or gave false answers. With all that being said, the research results cannot be used for generalization to the entire banking sector of Kazakhstan.

4.8 Data Analysis

This study sought to comprehend the phenomena of how these small groups of participants made sense of their experience, and to extend self experience that the researcher aspired to increase. The analysis of the collected data was based on the write-up notes taken during the interviews with the participants. The findings of each group interviews were examined and analyzed separately, forming different categories of findings and emphasizing how they affected the researcher's experience on the studied topic.

4.8.1 Data Analysis for Research Question 1

The below open-ended questions in "Group II – Bank Employees" interview were used to obtain data for answering Research Question 1 (RQ1), "To what extent, if any, is privacy of credit card and cardholder data considered and implemented in the banks of Kazakhstan?" (See Appendix C).

1. Do you know what laws, regulations or standards, if any, exist in the sphere of security and privacy of credit card and cardholder data in Kazakhstan?
2. Does your bank comply with these laws, regulations and standards?
3. Have you heard of such laws, regulations or standards being used in foreign countries?
4. What international payment cards does your bank issue?
5. Have you heard about Payment Card Industry Data Security Standard (PCI DSS) of the U.S., which was created to help financial organizations protect credit card and cardholder data? Is it considered and being implemented in your organization?
6. What organization, if any, is auditing your bank for being compliant with regulations per privacy of credit card and cardholder data? How often does it happen?
7. Does your bank send out card-statements to its customers? Are they sent via postal mail, e-mail or SMS (mobile banking)? What kind of banking information is included in such report? Does your bank encrypt traffic that is sent over public networks?

4.8.2 Data Analysis for Research Question 2

The below open-ended questions in "Group II – Bank Employees" interview were used to obtain data for answering Research Question 2 (RQ2), "What is the banks' level of data privacy awareness? How well do they understand the importance of data privacy?" (See Appendix C).

1. What is defined under the term “personal information”? Do you think this term includes banking information?
2. Are confidentiality and integrity of your customers’ credit card data important for your bank? How are they addressed in your organization?
3. Are you familiar with the term “data breach”? Do you think data of your customers could be “breached” and get compromised (disclosed)? If this occurred, would the clients and public (via media) be informed (notified) about it? Would your bank announce a cause and estimated damage of the breach?
4. Do you think your consumers’ data is well protected from internal/external abuse?
5. Do you know how your bank uses and shares credit card and cardholder data internally and externally? What internal standards/rules regulate it? Are you familiar with them?
6. By your opinion, what aspects of security of privacy information should your bank strengthen, and why?

4.8.3 Data Analysis for Research Question 3

The below open-ended questions in “Group III – Bank Customers” interview were used to obtain data for answering Research Question 3 (RQ3), “To what extent, if any, are the bank customers concerned about privacy of their credit card and cardholder data?” (See Appendix D).

1. Do you know what is defined under term “personal information”? Does it have to be confidential? Do you think your banking information has to be confidential as well?

2. Have you heard of any laws or regulations that exist in Kazakhstan to protect credit card and cardholder data? Do you think your bank is aware of them and compliant with them? Do you know of such laws/standards in other countries?
3. Are you familiar with your rights of using own banking information (provided in the terms of use that you have signed with your bank)? What are their basics?
4. Are you familiar with the rules of how your bank uses and shares your banking information internally? What are they?
5. Are you familiar with the rules (conditions) of how and to whom your banking information could be revealed outside of your bank? What are they?
6. Do you trust your bank in terms of providing a proper level of security of your banking information?
7. Have you received, if at all, your card statements via mail, Internet or SMS (mobile banking)? If so, what kind of banking information was included in there?

5. RESULTS

5.1 Overview

This chapter of the study presents the findings to the research questions from the interviews with the participants. First, the banking sector has a critical deficiency in consideration and implementation of data privacy. Second, there is a necessity to implement security and privacy-awareness trainings and programs for bank employees. Third, financial institutions, i.e. banks in particular, should ensure customers' understanding of data privacy and its requirements. The discussion of each result is provided further.

5.2 Research Question 1

Question statement (RQ1): To what extent, if any, is privacy of credit card and cardholder data considered and implemented in the banks of Kazakhstan?

Findings and interpretations: The questions of the section 4.8.1 addressed to the second focus group – bank employees, presented the primary data for RQ1 of this study, and full interviews with the participants of that group could be found in Appendix C. The questions, which are included in the interviews of Appendix C but were not included in the section 4.8.1, have presented the secondary data to support or contradict the primary one. The information collected from the interviews with the first focus group – lawyers (Appendix B), was also included into the primary and secondary data. The bank employees group consisted of eight respondents, who were employed

at the moment of interviews and held positions within the credit card departments of different banks in Kazakhstan.

According to the interview results, privacy of credit card and cardholder data was poorly considered and implemented. Surprisingly, there was no appropriate legislation in Kazakhstan that would regulate security and privacy of customers' financial data, i.e. credit card and cardholder data [Appendix B, C]. All existing legal framework that was somewhat related to the security and privacy of financial information introduced some general basics, not being sophisticated enough to cover this delicate topic in-depth. An examination of the current legislation did not provide any prime example of a separate law or regulation to be dedicated to privacy of financial information. A founded government regulation approved the list of individual's data, declared to be personal, which, however, did not include individual's banking information (The Government Regulation, 2007). All participants referred to the state laws (The Law of the Republic of Kazakhstan No. 2155, 244, 474 and the Civil Code) in response to the question about known legislation in the sphere of privacy of credit card and cardholder data that their organizations complied with. Seven out of eight respondents were not aware of PCI DSS, while only one person noted that he has heard of it. Consequently, none of them could tell whether the requirements of PCI DSS were considered and implemented in their organizations or not, even though they issued payment cards of such brands as Visa Inc., MasterCard, American Express, who were among the main card brands comprising the PCI Security Standards Council and behind the development of PCI DSS.

One of the main interview questions inquired about sending card-statements to cardholders via postal mail, e-mail or SMS (mobile banking), and what information was included therein. One respondent did not have sufficient information to answer this question, and another one noted that her bank provided card-statements to its cardholders in person only. At the same time, the remainder of the respondents confirmed that their bank's payment application facilitated card statements, which were sent via e-mail, and the statements included cardholder's full name, SSN and payment card number. Per the question of encryption applied to the sensitive traffic sent over public networks, only a few respondents believed that it was encrypted.

Overall, consideration and implementation of privacy of credit card and cardholder data in the banks was low. Privacy of customers' data was not addressed properly and significant violations took place. PCI DSS was not a part of the banks security practices; consequently, the participants were not aware of their organization's obligation under it. Also, the results of the interviews indicated that there was no auditing of the banks for being compliant with regulations per data privacy, in particular. In fact, if such regulations do not exist on the state or organizational level, there is no legal reason, nor need for auditing to occur.

5.3 Research Question 2

Question statement (RQ2): What is the banks' level of data privacy awareness? How well do they understand the importance of data privacy?

Findings and interpretations: The questions of the section 4.8.2 addressed to the second focus group again – bank employees, have presented a primary data for RQ2

question of this study, and full interviews with the participants of that group could be found in Appendix C. The questions, which are included in the interviews of Appendix B but were not included in the section 4.8.2, have presented the secondary data to support or contradict the primary one. Both 4.8.1 and 4.8.2 sections have a few crossed questions addressing RQ1 and RQ2 of this study. This is why the information collected for RQ1 was referred to and used to some extent when answering RQ2.

Overall, all participants showed a good understanding of what “data breach” and “personal information” are, indicating that credit card and cardholder data is certainly included in the term of personal information, hence, is to be safeguarded as well. At the same time, when asked whether they think that credit card and cardholder data of their customers was well protected from internal/external abuse, five out of eight participants responded negatively referring to employees as the major obstacle in achieving security of such data, since employees often have unlimited access to this sensitive data and could easily partner with unauthorized parties to compromise it in exchange for own benefit. According to some respondents, misuse of credit card and cardholder data by employees had happened in their banks before. Only one respondent thought that credit card and cardholder data was well protected in his organization, and believed that an agreement not to disclose highly confidential and proprietary data (such as trade secrets, financial data and other sensitive information, including an ethical obligation to protect cardholders’ data), which has to be signed by all employees, is a good preventive measure against any internal abuse of sensitive information. Other two respondents (interviews of Respondents C7, C8) declined to answer this question at all, considering it a disclosure of their banks’ confidential information.

The responses to the questions per organization's security policies and rules that regulate internal or external access, use and share of credit card and cardholder data indicated that the participants knew that such policies and rules existed in their organizations, but no one could name at least one policy/rule and explain what aspects of data privacy they covered.

Not specifying any internal policy or rule per security and privacy of credit card and cardholder data, all participants, however, excellently knew state laws and regulations that were somewhat related to the subject of data privacy. At the same time, interviews with the lawyers (Appendix B) and further analysis of the related legislation (Chapter 3, Section 3.2) indicated that those laws and regulations are insufficient and do not cover security and privacy of credit card and cardholder data. This uncommon correlation between not knowing one's own data privacy policies and instead state laws and regulations raises the questions of whether bank employees have an adequate understanding of data privacy concerns and requirements, and whether their organizations have such policies at all. The reasoning behind the former might be due to the lack of supervisory work that would have ensured employees' awareness and understanding of data privacy. The reasoning behind latter question could be explained by the respondents' commitment to their organizations, meaning that they deliberately hid the absence of policies regulating data privacy in their organizations in an attempt to make their organizations "look" good. There is also a high probability that the respondents did not provide adequate information in the fear that it would affect their further career and employment.

Thus, based on these findings, the level of bank employees' data privacy awareness was low as well. None of the interviewed employees had trainings on security and privacy of cardholders' data at the workplace. If they do not know what data privacy is and how it is implemented, they will not have understanding of it, or knowledge of the possible threats. Without it, they could not understand importance of data privacy and its available countermeasures, and consequently, they could not provide security and guarantee privacy of credit card and cardholder data.

5.4 Research Question 3

Question statement (RQ3): To what extent, if any, are the bank customers concerned about privacy of their credit card and cardholder data?

Findings and interpretations: The questions of the section 4.8.3 addressed to the third focus group – bank customers, have presented the primary data for RQ3 of this study, and full interviews with the participants of that group could be found in Appendix D. The questions, which are included in the interviews of Appendix D but were not included in the section 4.8.3, have presented the secondary data to support or contradict the primary one. All three sections, 4.8.1, 4.8.2 and 4.8.3, have a few intersecting questions, which addressed participants' acquaintance with data privacy and the legislation regulating it. The data collected for RQ1 and RQ2 was referred to and used to some extent when answering RQ3. The bank customers group consisted of 6 respondents, who were Kazakhstan citizens and consumers of Kazakhstan banks' services at the time of interviews.

Generally, the respondents were able to define what “personal data” was, and what main components it had, indicating that their banking information was certainly a part of it, thus needed to be kept confidential. At the same time, none of the respondents knew of any law or regulation per privacy of credit card and cardholder data enacted in the state. Only two respondents knew foreign country’s data privacy legislation, which were the Sarbanes-Oxley Act (SOX) and PCI DSS of the USA. However, all of the respondents believed that if privacy legislation existed in Kazakhstan, their banks were surely aware of and in compliance with them.

A discouraging finding is that the vast majority of respondents were not familiar with their rights associated with using their own banking information, provided in the terms of use by their banks. As the respondents stated, they either had no motivation or need to read the agreement or could not recall what was there. They also had no interest in learning how their banks used and shared their banking information internally or under which conditions it might be revealed to third parties. In this respect, all the customers simply trusted their banks stating that they should know how to do the right thing.

In addition, the customers were asked whether they were receiving their card-statements through mail, Internet (email) or SMS (mobile banking). While a half of the respondents used online banking, another half stated that they have been receiving a card-statement via email and confirmed that it contained the cardholder’s full name, SSN and payment card number along with other information. There was little, if any, concern amongst the participants about having all this data in the card-statement sent via email.

Overall, the customers' segment was clearly divided into two different groups based on their concerns about privacy of their data: they either completely trusted their banks and believed that the banks know what to do right – here is a default perception to rely on others rather than taking a part of responsibilities; or they were completely indifferent, but not until after something bad happens – here is a clear tendency to learn from experience, especially negative. Outcomes of these interviews to some extent correlated with the findings of Tsarenko and Tojib's research that validated a financial customer cluster based on their privacy concerns, revealing three different customer segments: the pragmatist, indifferent, and competent (p. 476).

6. IN CONCLUSION

6.1 Implications

The research indicated that Kazakhstan banks were referring to the state laws and regulations that were not sufficient, nor sophisticated enough, to provide an effective guidance in securing privacy of credit card and cardholder data. The results demonstrated that comprehensive privacy legislation, reflecting what personal data is, how and by who it is to be protected needs to be created in Kazakhstan. Its absence only worsens the current situation, increasing risks of data breaches and credit card fraud, as the financial institutions did not have privacy legislation to refer to when addressing current issues. Hence, it was not surprising that the banks lacked consideration and implementation for the privacy of credit card and cardholder data in their practices. The growing trend in the international practice advises financial institutions to develop and implement their own data privacy policies and rules to possibly prevent compromise of personal information and identity theft. In fact, financial organizations that partner with such payment brands as American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. must comply with their PCI Data Security Standard. Foremost, there should be an authorized organization that will be in charge for auditing financial organizations for compliance with created privacy legislation. After privacy legislation is enacted, the government of Kazakhstan should enforce compliance with it, applying necessary penalties for its abuse.

The question of banks' data privacy awareness and understanding of its importance is to be addressed next, as the research findings proved it to be another serious issue. It is a common misperception that only IT professionals should be knowledgeable regarding data privacy concerns, practices and their implementations. However, bank customers rely on their banks and bank employees in particular, for instructions regarding privacy of their data. Bank employees' ignorance of data privacy may result in severe financial damages, legal issues, loss of bank's reputation and trust of its customers. In this respect, organization of workshops and trainings for employees, involving experience exchange with international experts, agencies and foreign countries would help local auditing and financial organizations better understand current practices in data privacy.

Customers' data privacy awareness and factors driving their concerns are another issue to be worry about. As the research results demonstrated, there were two different segments of the customers' group: those, who relied on the banks regarding their data privacy; and those, who were indifferent, stating that they would not get concerned until after a privacy breach occurred. However, ignoring and not understanding how their personal information is collected and used makes the achievement of data privacy harder and risks of its compromise larger. Thus, it is crucial to help customers enhance their data privacy knowledge and develop privacy concerns: less alert they are – more chances to have their personal information breached. Customers need to be involved into security awareness educational programs organized with the help of the government and financial institutions. Also, an open dialog between banks and their

customers would help to strengthen their relationship to better address existing data privacy concerns and understand its requirements.

6.2 Recommendations

Based on the collected data and findings of the research, the following recommendations are suggested:

1. Comprehensive privacy legislation to be developed and enacted in the country. Adoption of international standards, cooperation and experience exchange with foreign agencies and countries will be helpful in this regard.
2. Government and businesses should collaborate to establish a special committee that will be authorized to audit all financial institutions for being compliant with the new privacy legislation.
3. Data privacy standards restricting controls over personal data and providing better assurance of its security to be created and implemented on enterprise level. Necessary educational trainings for personnel to better understand importance of data privacy and adequately address its existing concerns to be included.
4. Better communications with customers to comprehend their concerns and provide better services to ensure a maximum security over their financial data. Level of customers' privacy awareness will be increased, if they have more knowledge and understanding regarding privacy of their financial information. Thus, customers' data privacy awareness, training and education are as much important as those of bank employees.

6.3 For Future Research

Future research should be targeted to a wider sample of population, using a quantitative or mixed approach to get a better observation and understanding of the studied phenomenon. It also should identify IT professionals' perceptions of data privacy concerns and requirements, and determine how they align or misalign with those of their international colleagues and what their role in protecting customer information is. The researcher believes that these findings would greatly contribute to the body of the present study, thus, establishing basis for further research on the current problem and prerequisites for future development of adequate legislation on data privacy in Kazakhstan.

BIBLIOGRAPHY

The Civil Code of the Republic of Kazakhstan. (1994, December 27). Retrieved from Republic of Kazakhstan website: http://www.damu.kz/content/files/FullVersion_2.doc

Creswell, J. W. (2003). *Research design* (C. D. Laughton, V. Novak, D. E. Axelson, & A. J. Sobczak, Eds., 2nd ed.). Thousand Oaks, CA: SAGE. (Original work published 1994)

General information about the Republic of Kazakhstan. (n.d.). Retrieved September 21, 2010, from http://akorda.kz/en/kazakhstan/general_information/general_information_about_the_republic_of_kazakhstan

The government regulation of the Republic of Kazakhstan No. 460 "On approving of the list of personal data of individuals included in the government electronic information resources". (2007).

Kasera, S. (2007, Winter). *Kazakhstan: Economic policies before and after the 1998 Russian financial crisis*. Retrieved from Stern School of Business, New York University website: http://cs.nyu.edu/~sk1759/Kazakhstan.pdf

The Law of the Republic of Kazakhstan No. 237-I "On payments and funds transfers." (1998).

The Law of the Republic of Kazakhstan No. 370-II "About electronic documents and electronic digital signature in the Republic of Kazakhstan." (2003).

The Law of the Republic of Kazakhstan No. 474 "On the State's financial regulation and supervision of the financial market and financial organizations.". (2003).

The Law of the Republic of Kazakhstan No. 2444 "About banks and banking activities in the Republic of Kazakhstan." (est. Apr.1993; revised Aug. 1995)

The Law of the Republic of Kazakhstan No. 2155. (1995, March). Retrieved September 20, 2010, from National Bank of the Republic of Kazakhstan website: http://www.nationalbank.kz/cont/publish588098_6516.doc

Lyakhov, A. E. (2002). *Банковская система Республики Казахстан* [Banking system of the Republic of Kazakhstan]. Retrieved from http://www.lyakhov.kz/iguide/03/iab0302.shtml

McCallister, E., Grance, T., & Scarfone, K. (2010, April). *Guide to protecting the confidentiality of personally identifiable information (PII)* [Special publication 800-12]. Retrieved from National Institute of Standards and Technology, U.S. Department of Commerce website: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

The National Bank of the Republic of Kazakhstan No. 400 "Instruction to requirements to software and hardware which provide access to payment system of Republic of Kazakhstan". (2000).

The National Bank of the Republic of Kazakhstan No. 146 "Rules of electronic documents exchange in committing of payments and money transfers in Republic of Kazakhstan". (2000).

The National Bank of the Republic of Kazakhstan No. 179 "Rules on the use of payment documents and accomplishment of non-cash payments and funds transfer in Republic of Kazakhstan.". (2000).

The National Bank of the Republic of Kazakhstan No. 32 "To the questions on the second-tier banks' transition to the international standards.". (2001).

The National Bank of the Republic of Kazakhstan No. 386 "Procedures of resolving conflicts regarding authenticity of electronic documents in the payment system of Republic of Kazakhstan". (1999).

The National Bank of the Republic of Kazakhstan No. 325 "Rules provisioning security of operator's working place of payment system participants of the state enterprise Kazakhstan Interbank Settlement Centre of the National Bank of the Republic of Kazakhstan.". (1999).

The National Bank of the Republic of Kazakhstan No. 242 "Rules of funds transfers in the Interbank System of Money Transfers.". (1998).

The National Bank of the Republic of Kazakhstan No. 292 "Regulations on the second-tier banks' transition to the international standards". (1996).

On the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995, October 24). *Directive 95/46/EC of The European Parliament and of the council*. Retrieved from International Congress of Mathematicians website: http://www.icm2006.org/imgs/congresos/Directive%2095%2046%20EC.pdf

Payments and securities clearance and settlement systems in Kazakhstan [Public disclosure document]. (2006, April). Retrieved from The World Bank website: http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2008/09/05/000334955_20080905071747/Rendered/PDF/452290WP0Box3410securities01PUBLIC1.pdf

Report and recommendation of the president to the board of directors [Proposed assistance to Private Bank in Kazakhstan]. (2005). Retrieved from Asian Development Bank website: http://www.adb.org/Documents/RRPs/KAZ/40908-KAZ-RRP-01.pdf

Requirements and security assessment procedures. (2010, September 28). *Payment Card Industry (PCI) Data Security Standard version 2.0*. Retrieved from PCI Security Standards Council website: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

Tsarenko, Y., & Tojib, D. R. (2009). Examining customer privacy concerns in dealings with financial institutions. *The Journal of Consumer Marketing, 26*(7), 468-476. Retrieved from ABI/INFORM Global database. (1919986861)

Wang, H., Lee, M. K. O., & Wang, C. (1998, March). Consumer privacy concerns about Internet marketing. *Communications of the ACM, 41*(3), 63-70. doi:10.1145/272287.272

APPENDICES

A. Informed Consent Form

INFORMED CONSENT FORM

for the research study on

DATA PRIVACY: LEGAL AND BUSINESS MALPRACTICE

by

GULMIRA ZHAVGASHEVA
MS Candidate

Research Purpose: To evaluate the extent, to which privacy of credit card and cardholder data is considered and implemented in the banking sector of Kazakhstan. The research also seeks to explore perceptions of banks (as in bank employees) in terms of data privacy awareness and their understanding of its significant importance, as well as concerns of bank customers in terms of privacy of their banking information.

Research Value: The findings will greatly contribute to the existing body of the literature, establishing basis for further research on the current problem and prerequisites for future development of adequate legislation on data privacy in Kazakhstan.

Sample Population: The research targets three focus groups of participants – lawyers, bank employees and bank customers (consumers).

Research Terms and Conditions: You will participate in an interview with open-ended questions related to your work activities. You may or may not answer the questions you do not feel comfortable with or do not know the answers. Your name, job position and place of work, along with the interview results will remain anonymous and only be used for the purpose of this research, not being shared with or disclosed to third parties.

Name Signature Date

_____

Researcher

_____

Participant

B. Interviews with Lawyers

Respondent B1

1. **How do you define term "personal information"?**
   I understand it as "personal information." Personal information is: first, middle and last names; place and date of birth; address; social and marital status; education; passport number, SSN.

2. **Do you know if there are any laws and regulations regarding privacy of credit card and cardholder data in Kazakhstan? What are they? Do institutions have to be in compliance with them?**
   I'm sure, such laws and regulations exist, I just don't know what they are… But every bank has its own acts and rules regarding security and privacy of personal information… All entities that operate on the territory of Kazakhstan have to comply with the state legislation.

3. **Have you heard of such international legislation?**
   No, I haven't.

4. **Is it forbidden to adopt international regulations or standards for Kazakhstan's legislation, if need be? Whose initiative it is to be?**
   No, it's not forbidden at all. It usually happens under initiative of administrative bodies. For example, when the Law on "Private Enterprise" was being revised to have new updates and amendments in it, the part regarding their auditing was developed with the help of international experts.

Respondent B2

1. **What is defined under term "personal information"?**

   The Government regulation of the Republic of Kazakhstan N460, of June 5, 2007, "On approving of the list of personal data of individuals included in the government electronic information resources," provides a definition of personal information, such as individual's last name, first name, middle name; date and place of birth; nationality; gender; marital status; citizenship; unique identification number [which is a passport number]; photograph; address.

2. **Are there any laws and regulations regarding privacy of personal information, enacted in Kazakhstan? What are they?**

   Yes, we have this kind of laws and regulations. For example, the Constitution of the RK, Article 18 states that:

   1. Everyone has the right to privacy, personal or family secrets, protection of honor and dignity.
   2. Everyone has the right to confidentiality of personal deposits and savings, correspondence, telephone conversations, postal, telegraphic and other communications. Restrictions on this right shall be permitted only in cases and in the manner expressly provided by law.
   3. State bodies, public associations, officials and the media must provide every citizen the opportunity to get acquainted with concerning his rights and interests of documents, decisions and information sources.

3. **Is it mandatory for any institution to comply with such legislation?**

   Yes, any entity that resides and/or does business within Kazakhstan borders has to be in compliance with them. Furthermore, any organization must develop and implement their own measures to keep their information secure.

4. **Is it forbidden to adopt international regulations or standards for Kazakhstan's legislation, if need be? Whose initiative it is to be?**
   Yes, it [adoption] happens in the jurisprudence of any country. We do that too, if it is needed and reasonable.

Respondent B3

1. **How is "personal information" defined in our legislation?**
   There's the Government regulation N460, "On approving of the list of personal data of individuals included in the government electronic information resources," which gives a definition of what personal information is: last, first and middle name; date and place of birth; nationality; gender; marital status; citizenship; unique identification number; photograph; address; signature; passport data. I think that bio-data, such as fingerprints, needs to be in that list as well.

2. **Do you know what laws, regulations or standards, if any, exist in the sphere of security and privacy of credit card and cardholder data in Kazakhstan? Are you familiar with such legislation in other countries?**
   Such legislation exists in all countries. Don't know any international law in particular, but for Kazakhstan they are as follow: the Constitution, the Laws on National Security, National Bank, Banks and Banking Activities.

3. **Do organizations have to be in compliance with these laws? How is this to be checked?**
   Yes, all organizations that have any business activities in Kazakhstan have to comply with the state laws. There are special agencies for a certain field (they act in accordance with the Ministry they work under) that audit institutions for all sort of things. I think in case of financial activities, the Financial Markets Supervisory Agency will be in charge for auditing and supervising institutions.

4. **How are international regulations to be adopted? Whose initiative it is to be?**

   International best practices and experience are always good to look at, when developing own regulations. When administrative bodies are in the process of creating some law or regulation, and a similar international law already exists, it would be considered in our practice, if need be.

Respondent B4

1. **What is "personal information"?**

   It's any personal data that is not meant to be publicly available or shared.

2. **Do you know what laws, regulations or standards, if any, exist in the sphere of security and privacy of credit card and cardholder data in Kazakhstan? Were any of them adopted (wholly or partially) from the international laws and practice?**

   The statements per privacy of personal information (including banking information) are declared in such laws as: Constitution, Civil Code, About National Bank, Banks and Bank Activities. I don't think they were adopted.

3. **Do organizations and what kind of them have to be in compliance with these laws/regulations/standards, or it's not mandatory at all in Kazakhstan?**

   Financial organizations, in particular, must comply with legislation per their activities, including the times, when it comes to security and confidentiality of customer's banking information.

Respondent B5

1. **What is "personal information" per Kazakhstan's legislation?**
   Per the Government regulation, it is " an individual's full name; date and place of birth; nationality; gender; marital status; citizenship; passport number; photograph; address."
   We also have term "employee's personal data," defined by the Labor Code as information about employee and is needed for origination, continuation and termination of his/her employment.

2. **How about your banking information, such as payment card numbers, account's balance, etc. – do you consider this data to be personal as well?**
   Yes, of course, this data is personal too, and needs to be protected just like any other private information.

3. **Do you know what laws and regulations exist in Kazakhstan per security and privacy banking information? Do banks or other financial institutions have to be in compliance with them?**
   I don't know of any law specifically dedicated to it, but I would think that its security and privacy should be covered by the Law on the National Bank of the Republic of Kazakhstan, and the Law about Banks and Banking Activities in the Republic of Kazakhstan. Yes, if there're such laws and regulations, then all financial institutions have to be in compliance with them.

4. **How is a new law or regulation to be developed and enacted in Kazakhstan? Whose initiative it is to be?**

a) It is to be developed by those institutions, whose activities it might affect.
b) The draft is sent for approval to the institutions (ministries, agencies), who are interested on this subject. The Ministries of Jurisprudence and Finance have to be in an approval flow of any project document.

c) After the draft has been revised to include approvers' notes/points, the project document is sent to the Minister of that administrative body.
d) If the project document is within the interests of business entities, it will also be sent to them for more editing/information.
e) After it's been finalized and approved, the project document is sent to the Prime-Minister's Office (PMO) for further discussion and expertise. All disagreements, if any, will be put into a protocol of disagreements, which are to be solved through further discussions in the PMO. The protocol will also be sent to the Administration of the President.
f) After all disagreements were dissolved, the project document will be presented to the Parliament, and if they vote for it, the project document will be signed and considered active.

Respondent B6

1. **How do you define term "personal information" according to existing legislation?**

   It's a personal data, using which makes it possible to identify a physical person (individual).

2. **Do you know what laws and regulations, if any, exist in the sphere of security and privacy of credit card and cardholder data in Kazakhstan?**

   There are several laws and regulations that have clauses about data privacy and its security. However, I can't tell whether these clauses were adopted from the international practices or not. As of security and privacy of personal data, the Civil Code's Article 745 is about bank secrecy. It states that bank assures confidentiality of individual's bank secrecy. The list of data that comprises bank secrecy and terms of its disclosure are defined by a legislation that regulates bank's activities. Article 126 states that the civil legislation secures information, defined as proprietary or trade (commercial) secret in case, if it has an actual or potential trade value being unknown to third parties, with no public access to it by any law, and an owner of the information undertakes measures to keep it secure

and confidential. With that being said, organizations have to develop and implement own regulations and rules per data privacy, in addition to the existing legislation.

3. **How to determine whether financial institutions comply with these laws and regulations?**

   I assume that the Financial Markets Supervisory Agency would be in charge for financial auditing and monitoring of financial institutions. Unfortunately, I don't know any exact procedure for that matter.

4. **Do you know if there are any laws or regulations adopted from the international practices related to data privacy?**

   No, I don't know about it.

5. **What's the procedure for having a new law/regulation developed and enacted?**

   a) It is to be developed by those institutions, whose activities it might affect.
   b) The draft is sent for approval to the institutions (ministries, agencies), who are interested on this subject. The Ministries of Jurisprudence and Finance have to be in an approval flow of any project document.
   c) After the draft has been revised to include approvers' notes/points, the project document is sent to the Minister of that administrative body.
   d) If the project document is within the interests of business entities, it will also be sent to them for more editing/information.
   e) After it's been finalized and approved, the project document is sent to the Prime-Minister's Office (PMO) for further discussion and expertise. All disagreements, if any, will be put into a protocol of disagreements, which are to be solved through further discussions in the PMO. The protocol will also be sent to the Administration of the President.
   f) After all disagreements were dissolved, the project document will be presented to the Parliament, and if it gets more votes, the project document will be signed and become active.

Respondent B7

1. **Are you familiar with term "personal information"? What's included in it?**
   The following data of a physical person – first, middle, last name; SSN; passport data; Social Individual Number; place and date of birth; gender; marital status; address; citizenship – is defined under term "personal information."

2. **What laws and/or regulations guarantee security and privacy of credit card and cardholder data exist in Kazakhstan? Is there any of laws or regulations being adopted from international practice?**
   Well, the Laws about "Bank Secrecy" and "About Banks and Bank activities" state that bank secrecy includes information about accounts, cardholders, payment card numbers, card-statements, money flow of bank itself and its customers, bank operations, as well as information about value and price of customers' property that is stored in bank. Also, banks guarantee secrecy of the operations, accounts and deposits of its customers and correspondents, as well as secrecy of the property that is stored in bank. So, I think those are the laws that address privacy issues.

3. **Shall organizations in Kazakhstan comply with these laws and regulations?**
   Yes, definitely. But different organizations might need to comply with different laws and regulations, depending upon organization's business activities.

4. **Have you ever been a part of the work group, whose responsibility was development and adoption of some international laws or regulations to contribute to Kazakhstan's realities?**
   No, I haven't.

Respondent B8

1. **Can you please explain what "personal information" is?**
   Personal information is a private data of physical person.

2. **What does that private data include?**

   Well, it is: person's full name, date of birth, passport number, SSN and his banking information. A full list of personal information you can obtain from the Government regulation N460, "On approving of the list of personal data of individuals included in the government electronic information resources."

3. **What laws and regulations guarantee security and privacy of personal information?**

   I think that this problem is regulated by the following laws: About Bank Secrecy, About Banks and Bank activities, Constitution, Civil Code, About National Bank.

4. **Do organizations in Kazakhstan have to be in compliance with these laws and regulations? What organization, if any, has authority to control and audit other organizations for being compliant?**

   Of course, all organizations must comply with such legislation and do their business in accordance with it. I don't know for sure, who has such responsibilities to audit other organizations, but I think such institutions, as police, finance police, banks and health institutions should be in compliance with privacy regulations by default.

5. **What's the procedure for developing and enacting a new law, regulation or act?**

   Article 7, in The Regulations of Administration of the President of the Republic of Kazakhstan, N11/90, August 18, 2006, explains the entire procedure in all needed details.

6. **How about adoption of international standards or practices – does it happen in our legal sector?**

   Yes, we practice adoption of international standards, if need be. Administrative bodies and state agencies decide it themselves, which regulation/standard to be adopted and what parts of it would better suit our country.

Respondent B9

1. **What is "personal information"?**

   According to the Government regulation N460, "On approving of the list of personal data of individuals included in the government electronic information resources," it is "individual's full name; date and place of birth; nationality; gender; marital status; citizenship; passport number; photograph; address."

2. **Are there any laws or regulations per security and privacy of personal information enacted in Kazakhstan?**

   I think there is no such privacy legislation in Kazakhstan.

3. **Ok, if it does not exist yet, then what institution shall enact it?**

   I don't know, maybe it should be initiated by the Ministry of Finance or National Bank of Kazakhstan.

4. **How about adoption of international standards or practices – isn't it easier to do than developing a new one?**

   Yes, adoption of other countries' regulations and standards is a common thing worldwide. Normally, our administrative bodies and their agencies decide themselves, whether adopt (and to what extent) international regulations or standards or not.

C. Interviews with Bank Employees

Respondent C1

1. **What is defined under "personal information"? Is "banking information" included in it as well?**

   Personal information is a private data of physical person; it includes person's full name, date of birth, address, SSN, passport data (passport number, issued date, etc.), and banking information.

   Banking information could be: information about all customers of bank; information about bank's accounts and bank's operations; information about cardholders and their property that is stored in bank; etc.

2. **Do you know what laws, regulations or standards, if any, exist in the sphere of security and privacy of credit card and cardholder data in Kazakhstan? Do you know of such international legislation, like Payment Card Industry Data Security Standard (PCI DSS)?**

   Kazakhstan's privacy legislation – "Civil Code" and laws "About National Bank", "About Banks and Bank Activities" and "About Bank Secrecy." Unfortunately, I don't know anything about international privacy legislation – no, I don't know about PCI DSS either.

3. **Does your bank comply with the mentioned laws?**

   Yes, of course. Activity of any organization must go only in accordance with the national legislation.

4. **Who (what organization) does audit your bank for being compliant with the mentioned legislation? How often does it happen?**

   It's done by the Financial Markets Supervisory Agency once a year. Also, there are independent auditing organizations that are licensed for auditing and could

audit a bank, if the latter hires them to do so. Banks, themselves, maintain an internal audit, which could be held on different schedules.

5. **What international payment card brands does your bank issue?**
   They are Visa, Master Card and China Union Pay.

6. **Issuing this kind of payment brands should make your bank seeking for compliance with PCIDSS. Do you comply with PCI DSS?**
   No, I don't know anything about PCI DSS here, at work. Maybe management knows the answer better.

7. **What internal regulations per use, share of and access to cardholder's data do you have in place to ensure such data's security and privacy?**
   I only know of the Code of Conduct that all employees have to sign, if they are going to work here.

8. **Do you know to whom and how this credit card and cardholder data could be revealed outside of your bank? Do you think your customers know about it?**
   If there's an official request from administrative bodies (police, finance police, etc.) – we reveal it for the purpose of the request. Yes, I think our customers are aware of it.

9. **Does your bank send out card-statements (per account's balance) to customers? How is it sent: via postal mail, e-mail or SMS (mobile banking)? If so, what kind of cardholder information is included in there?**
   We send card-statements via e-mail, but a customer has to request it in a written form. Card-statements usually have money flow information, name of the customer, a time period it was for, SSN, account number.

10. **When sending out card-statements through open networks, does your bank encrypt it?**

I think it has to be encrypted. I don't have much information about it.

11. **Do you find sending card-reports via email a safe method of such sensitive data transfer?**

    Yes. I think it might not be safe at the user's end – if, for example, his/her mailbox was hacked, then hackers would get the customer's information.

12. **Do you think your customers' data is well protected from being abused internally?**

    No, I don't think so, because it's impossible to predict employee's behavior – we had a few cases, when our employees were involved into a credit card fraud or initiated it themselves.

13. **Do you know what "data breach" is? Do you think your customers' data could be "breached"? If so, then what could potentially cause it, in your opinion?**

    Yes, it's a leakage of confidential information. Yes, there's always a good probability to have any confidential data compromised. Especially, when there are many people, who have access to it for work purposes.

14. **Are there any security or data privacy awareness trainings available for employees at the workplace?**

    No, I don't think we have them at all. But I think IT department surely has them.

15. **If your organization's data was breached, would it inform the customers and public about it? What impact would the breach bring to the organization?**

    Yes, bank has to inform all customers who have been affected by the breach. I think, it will impact bank's reputation and budget, some customers and partners might re-consider a future relation and business with us.

16. **In your opinion, what aspects of data security and privacy does your organization need to pay a better attention to?**

    I think, access to customers' confidential information needs a better, as in more restricted solution. IT technology solutions must be always kept up to date. Also, I would suggest having awareness-training programs regarding privacy concerns and requirements for personnel.

Respondent C2

1. **What is defined under "personal information"? Is "banking information" included in it as well?**

   Personal information is data that can be used to define an individual: full name, date of birth, address, SSN, passport data (passport number, issued date, etc.), including banking information.

   Banking information could be: information about all customers of bank; information about bank's accounts and bank's operations; information about cardholders and their property that is stored in bank; etc.

2. **Do you know what laws, regulations or standards regarding to security and privacy of credit card and cardholder data exist in Kazakhstan? Do you know about international practices and standards?**

   I know only Kazakhstan's laws: "About Banks and Bank Activitie, "About Bank Secrecy" and The Civil Code. I know of PCI DSS, but I don't know its details.

3. **Does your bank comply with these laws?**

   Yes, definitely.

4. **Do you think your bank complies with PCI DSS as well?**

   I don't' think so. I didn't hear about PCI DSS at work though.

5. **What international payment cards does your bank issue?**
   We issue Visa and Master Card, along with local payment card brands.

6. **Who (what organization) is auditing your bank for being compliant with the mentioned legislation? How often does it happen?**
   It's done by the Financial Markets Supervisory Agency, once a year.

7. **What internal regulations per use, share of and access to cardholder's data do you have in place to ensure such data's security and privacy?**
   I think it's in the Code of Conduct. All employees also sign an obligation to Bank Secrecy.

8. **Do you know to whom and how this credit card and cardholder data could be revealed outside of your bank?**
   We provide this information to Police, Finance Police and Tax Services Agency, after they request it officially.

9. **Does your bank send out card-statements (per account's balance) to customers? How is it sent: via postal mail, e-mail or SMS (mobile banking)? If so, what kind of banking information is included in there?**
   Yes, we send card-statements via e-mail. When opening account, customer has to provide us his/her email address for receiving card-statements. Such card report contains customer's full name, date of report, reporting period, payment card number.

10. **Does your bank encrypt traffic that is sent over public networks? Do you know how it's implemented?**
    Yes, I believe traffic is encrypted, but I don't know details of it.

11. **Do you think your customers' data is well protected from being misused by bank employees?**

No, it's not. There's always a chance that sensitive data will be compromised. And the biggest threat is own employees. We try to restrict employees' access permissions, so that we don't have, for example, one employee with too many roles, which would mean too much permission. But the threat still exists – what if several employees decide to "collaborate" and "merge" their access permissions to misuse customers' data in some or another way. I think this problem will always stay current.

12. **Don't you have security-awareness and data privacy trainings/programs for your employees?**

    No, we don't. But it would be great, if we did.

13. **Are you familiar with term "data breach"? If your organization's data was breached, would your bank inform the customers and public about it? What impact would it bring to the organization?**

    Yes, I know what data breach is. If our bank's sensitive information was compromised and disclosed, we will notify all customers who suffered from this accident. I don't think that bank's administration would let people know that the breach occurred, for example, because of one of the employees – this will worsen bank's name and reputation. No one would like to have their business down or look unreliable; this is why sometimes it's better to keep such information in secret.

14. **In your opinion, what aspects of data privacy your bank needs to pay more attention to?**

    I think we need more internal regulations per data privacy. We also need to have all employees better understand all issues surrounding this topic. I think having a corporate spirit in the company (bank) will raise employees' responsibility and professionalism.

Respondent C3

1. **What is defined under "personal information"? Is "banking information" included in it as well?**

   Personal information is data that can be linked to a particular person only: his name, date of birth, address, SSN, passport number. Banking information – such as, credit story, debit/credit card numbers, number of bank accounts, available balance, etc. – is surely personal/private, and needs to be confidential.

   Banking information could be: information about all customers of bank; information about bank's accounts and bank's operations; information about cardholders and their property that is stored in bank; etc.

2. **What laws or regulations do you know regarding to privacy of banking information in Kazakhstan? Do you know such international laws?**

   It is the Law "About Banks and Bank Activities". But I don't know about international laws on the same subject.

3. **Have you heard about Payment Card Industry Data Security Standard of the U.S., which was created to help financial organizations protect credit card and cardholder data? If your bank issues such international payment cards as, Visa, MasterCard, Discovery, American Express – then your organization has to comply with this standard and implement its minimum requirements.**

   Yes, we issue Visa and MasterCard payment cards. But I've never heard about this standard. Maybe we implement it too, and I just don't know about it.

4. **What organization, if any, is auditing all financial organizations (banks, in particular) for being compliant with the financial legislation? How often does it happen?**

   The Financial Markets Supervisory Agency has authority for this kind of activity; they audit banks once a year, I believe. Or, maybe, twice a year.

5. **Does your bank have any internal regulations or rules per use, share of and/or access to cardholder's confidential data? What are their main principles, in short?**

   Yes, we employ policy on information security. I can't recall its details though; it's been a while since I've read it.

6. **Do you know to whom and how this credit card and cardholder data could be revealed outside of your bank?**

   We only provide such data to Police, Finance Police and Tax Services Agency - if we receive any official requests from them to do so. This information could also be shared with other bank, in case of two banks' union. I'm sure that more precise details could be found in the current laws and regulations – please refer to the Law "About Banks and Bank Activities" I mentioned earlier.

7. **Does your bank send out card-statements to customers, using postal mail, e-mail, or SMS notification?**

   No, we do not send card-statements to our customers. If the customer wants to have a card-statement, he/she needs to request and receive it in person.

8. **Do you think your customers' data is well protected from being misused by bank employees?**

   Yes, I think this data is well protected. All employees have to sign an obligation not to disclose any confidential information that they have access to for work purposes.

9. **Are you familiar with term "data breach"? If the bank's confidential information was compromised and stolen, would they inform all customers and public about it? What impact would it bring to your organization?**

   Yes, I'm familiar with this term. I don't know how my organization [bank] would act if data breach occurred to us. I also don't know whether my bank would want

to publicly announce about this incident – it will be hard to do so for sure, because data breach might become bank's disaster – it means lose of money, lose of partners, and lose of customers.

10. **And the last question for you. What aspects of data privacy, do you think your bank needs to address better?**
    I think we need to update current security systems; have more restricted access to the systems and better control over employees; and the last, but not the least aspect is to implement awareness-training programs for our employees to eliminate human error as much as possible.

Respondent C4

1. **What is defined under «personal information»? Is "banking information" included in it as well?**
   Personal information is a data that can be linked to an individual or legal entity. It definitely includes banking information.

2. **What laws or regulations do you know in regards to privacy of banking information in Kazakhstan? Do you know such international laws?**
   It is the Law "About Banks and Bank Activities." No, I am not familiar with such international legislation.

3. **What organization, if any, is auditing your bank for being compliant with the financial legislation? How often does it happen?**
   Banks are to be audited by own internal auditing services, Financial Markets Supervisory Agency, or international auditing organizations.

4. **Does your bank have any internal regulations or rules per use, share of and/or access to cardholder's confidential data?**

Yes, it has a policy on information security.

5. **Do you know to whom and how this credit card and cardholder data could be revealed outside of your bank? In your opinion, are your bank customers aware of it?**
   It can be provided by the official request of state authorities, or Financial Police. Our customers surely should know about it.

6. **Does your bank send out card-statements to its clients? Postal mailing or via Internet? If so, what kind of cardholder information is included in there?**
   I'm not aware of it.

7. **Do you think your customers' data is well protected from being misused by bank employees? What your organization does in order to prevent this from happening?**
   I think that customers' data is not well protected from such situations. And for now, our bank cannot provide the necessary protection – we need to have better controls over employees' access; also, security polices need to be more strict.

8. **If data breach occurred in our bank, would be customers and public notified about it?**
   Bank will not inform the public to avoid media attention that might ruin bank's reputation, but the suffered customers will surely know.

9. **What consequences might your bank and its customers face after data breach? And how would it impact your organization's information security patterns and practices further on?**
   Data breach incident would harm bank's reputation and might bring significant financial losses, etc. Information security patterns and current practices would be revised and become stricter. Probably, we would have some personnel changes – like, new managers, or rotation of people.

10. **What maybe a cause of data breach in your organization, in your opinion?**
    Most likely it may have own employees involved in it, as they have unrestricted access to the customers' data - there's a great chance to misuse it. Another reason of data breach could have been in a human error – for example, because of a new employee. Outdated IT systems or security polices – is also a possible cause of data breach.

11. **What variables does data privacy depend on, in your opinion?**
    I guess, they are information systems security and labor discipline of employees.

Respondent C5

1. **What is defined under «personal information»? Is «confidential banking information» included in it as well?**
   Personal information is a private data such as full name, SSN, identity information. Yes, it is included.

2. **What laws or regulations do you know regarding to privacy of banking information in Kazakhstan?**
   They are the Law "About Banks and Bank Secrecy," "About Banks and Bank Activities."

3. **Does your organization have to be in compliance with these laws/regulations/standards?**
   Surely, it has to.

4. **What organization, if any, is auditing your bank for being compliant with the financial legislation? How often does it happen?**
   I don't know anything about auditing.

5. **Does your bank have any internal regulations or rules per use, share of and/or access to cardholder's confidential data?**
   All employees have to sign a non-disclosure agreement, which should help to prevent such things from happening.

6. **Are there any educational training programs about privacy and security for employees?**
   No, I don't think we have such.

7. **Do you know to whom and how this credit card and cardholder data could be revealed outside of your bank? Please name the laws, regulations and standards, controlling this process. In your opinion, are your bank clients aware of these laws/regulations/standards?**
   Bank can reveal the private data by the request of Financial Police, Tax Services Agency, Prosecutor General, for investigation purposes. I'm not aware of any laws and regulations, controlling this. Usually, it's our management' responsibility. Our clients can get aware of this only upon their own initiative.

8. **Does your organization apply any requirements of the privacy rules that involve the use of cardholder data? If this is the case, does your organization make its employees follow these policies and procedures?**
   Yes, it, surely, does.

9. **Does your bank send out credit reports/statements to its clients? Mailing or via Internet? If so, what kind of cardholder information is included in there?**
   Yes, it does via internet. It has customer's name, his card number, date of report period, shows money flow, etc.

10. **Considering sending such reports via postal mail or internet, which way is less secure?**
    Internet.

11. **Do you [your bank] implement traffic encryption then?**

    I don't know. If it's supposed to be like that, then we probably do it.

12. **Do you think your customers' data is well protected from being misused by bank employees?**

    It's not protected well.

13. **Do you think, e there any data breaches involving compromise/disclosure of cardholder data and its harmful misuse possible to happen with your bank?**

    Yes, I think no one is protected from such incidents.

14. **If this would occur, will be customers and public informed about incident?**

    Yes, bank will inform customers, but only those, whose data was damaged.

15. **What consequences will your organization and its clients face after dealing with this breach?**

    It will harm bank's reputation; we might lose a lot of money too. And customers will be complaining.

16. **In your opinion, what aspects of privacy data your bank needs to pay attention?**

    Probably information systems would appear outdated.

Respondent C6

1. **What is defined under "personal information"? Is "banking information" included in it as well?**

Private data of a physical person is personal information, which is comprised of: first, middle, last names, date and place of birth, living address, SSN, passport data.

Banking information is personal information as well. It contains data about personal banking account(s), banking operations, i.e. all data per person's banking activity.

2. **Do you know what laws and regulations regarding security and privacy of credit card and cardholder data exist in Kazakhstan? Is there any regulation adopted from the international practice?**

   I don't know about adopted ones, regarding privacy of banking information, but the following legislation of the Republic of Kazakhstan – the Civil Code, laws "On National Bank," "About Banks and Bank Activities" and "About Bank Secrecy" have related articles and statements.

   The National Bank develops and enacts regulations and rules that are mandatory for implementation by other banks of Kazakhstan.

   I am sure that other countries have such a special legislation. Besides, I think that their level of security and privacy of banking information is more reliable and sophisticated than ours.

3. **So, does that mean that your bank should comply with these laws?**

   Yes, the bank definitely should comply with legislation.

4. **Is your bank being audited for compliance with any financial law/regulation? Who is an auditor in this case? How often does auditing happen?**

   Yes, our bank has to be audited time to time. An auditor could be a financial auditing organization (from Kazakhstan) that is licensed for auditing of financial institutions. If bank wants or needs to be audited for compliance with international standards/regulations, it might invite an international auditing organization to be audited. Also, Kazakhstan's Financial Markets Supervisory Agency is also

responsible for auditing. I think a common period for auditing once or twice a year. It might also depend upon reasons for being audited.

5. **What international payment card brands does your bank issue? Have you heard anything about Payment Card Industry Data Security Standard, by the U.S.?**
   Here, we issue such brands as MasterCard, Visa, along with the local brands, of course. No.

6. **What internal regulations per use, share of and access to cardholder's data do you have in place to ensure such data's security and privacy?**
   I cannot name particular ones, but I know for sure that all our personnel's work and responsibilities are tied by the state or internal legislation.

7. **Do you know to whom and how credit card and cardholder data could be revealed outside of your bank? Do you think your customers know about it?**
   Article 50 of the law "About Banks and Bank Activities" has all details per this question.

8. **Does your bank send out card-statements (per account's balance) to its customers? How is it sent: via postal mail, e-mail or SMS (mobile banking)? And what kind of cardholder information is reflected therein?**
   We do send card-statements to our customers, if they are willing to receive them via Internet (e-mail). I think, in the Law "On Banks and Banking Activities," Article 50, 6-7, gives this information.

9. **Does your bank encrypt the traffic that is sent over open networks?**
   Yes, I believe it is encrypted. it has to be encrypted.

10. **Do you think your customers' data is well protected from being abused by bank employees?**

    Yes, I think this data is secured.

Respondent C7

1. **What is defined under «personal information»? Is banking information included in it as well?**

   Any information that is related to the individual (his passport information and other identity information, his private life, his background, his property).

2. **What laws or regulations do you know regarding to privacy of banking information in Kazakhstan? Do you know such international laws or regulations?**

   The Law "About Banks and Bank Activities." We also follow internal regulations and rules that are created by the bank itself or coming down from the National Bank of Kazakhstan. I don't know anything about such international laws/regulations.

3. **Does your organization have to be in compliance with these laws/regulations/standards?**

   Yes, we try to meet them. But we create most of them [internal rules, procedures and standards] by ourselves.

4. **What organization [or who], if any, is auditing your bank for being compliant with the financial legislation? How often does it happen?**

   Auditors visit us every year, especially, those from the headquarters of the bank. They check our compliance with the financial legislation and internal regulations/procedures.

5. **Does your bank have any internal regulations or rules per use, share of and/or access to cardholder's confidential data? What are they?**
   Bank has internal regulation and we try to be in compliance with it, but it mostly depends on the employee. I can't disclose this information to outsiders. If there's a need to know our internal regulations, it needs to be officially requested from the bank's administration.

6. **Do you know to whom and how this credit card and cardholder data could be revealed outside of your bank? What are they? In your opinion, are bank customers aware of these laws/regulations/standards?**
   Confidential information is being shared only with the authorized representative of a cardholder with the evidence of notarized power of authority. Customers probably don't know about them.

7. **How does your bank make sure that its employees strictly follow these internal regulations, policies and procedures (Q. 5, 6)?**
   Employees have to follow internal regulations/policies/procedures – because this is a part of their job.

8. **Does your bank send out credit reports/statements to its clients? Mailing or via Internet? If so, what kind of cardholder information is included in there?**
   It is necessary to fill out an application in any bank branch in order to receive statements via email. The statement contains credit and debit information, customer's name, card number, time period. There is no such an option as receiving them via postal mail.

Respondent C8

1. **What is defined under "personal information"? Is banking information included in it as well?**

Any information related to the individual (his passport information and other identity information, his private life, his background, his property)

2. **What laws or regulations do you know regarding to privacy of banking information in Kazakhstan? Do you know such international laws?**
   It is the Law “About National Bank”, “About Banks and Bank Activities” and Civil Code. No, I don’t need to know international laws – they don’t apply to us.

3. **Are you in compliance with these laws?**
   Yes, we have to comply with all laws that related to our activities.

4. **What organization, if any, is auditing your bank for being compliant with the financial legislation? How often does it happen?**
   The Financial Markets Supervisory Agency has authority for auditing and monitoring. I’m not sure, maybe once a year.

5. **Does your bank have any internal regulations or rules per use, share of and/or access to cardholder’s confidential data? What are they, can you describe in short?**
   We do have such regulations and rules, but they are to be introduced to employees only, since these regulations are for internal use only.

6. **Do you know to whom and how this credit card and cardholder data could be revealed outside of your bank? Please name the laws, regulations and standards, controlling this process. In your opinion, are your bank customers aware of these laws/regulations/standards?**
   The Law “About Banks and Bank Activities” should be covering this area. Customers may or may not know about these laws. Even though, the national legislation is always available to public.

7. **Does your bank implement security and privacy awareness training programs for its employees?**

   No. But this is what we need for our work, I think.

8. **Does your bank send out card-reports (statements) to its customers? Mailing or via Internet? If so, what kind of cardholder information is included in there?**

   Yes, we email it, if a customer requests it in his card application when opening an account. It has information about his money flow, for sure. I don't know what else could be there.

D. Interviews with Bank Customers

Respondent D1

1. **Do you know what is defined under term "personal data"? Do you think your personal data has to be confidential (secret)? Do you consider your banking information - i.e. your credit card and cardholder data – to be a part of your "personal data"? Do you think your banking information has to be confidential as well?**

   In my opinion customer's address, full name, date of birth, passport number, social security number, etc. are defined under the term "personal data". I think personal data has to be confidential. I also think that banking information is a part of "personal data" and it has to be kept confidential, because if any of this information is public it can result in fraudulent activities. Also it is my personal business on what and how I spend my money on and what type of transactions I perform.

2. **Have you heard of any laws, regulations or standards that exist in the sphere of security of banking information – i.e. credit card and cardholder data - in Kazakhstan? Can you name any of these laws, regulations, and standards? Do you think your bank needs to be in compliance with them? Do you know of such laws/standards practice in other countries?**

   I am not familiar with the laws and regulations in the sphere of security of banking information in Kazakhstan. However, I believe there is a law that none of the banking information can be disclosed without customer's permission. Banks have to be in compliance with these laws in order to stay in business. I am sure that in the United States these regulations do exist.

3. **If you have never heard of such laws and regulations in KZ, do you think they should exist in our legislation or be enacted?**

If these laws do not exist they should definitely be enacted, because without these regulations banks will be free to disclose any information regarding their customers. In such a case customer's personal information will be unprotected, which could lead to some illegal actions.

4. **Are you familiar with your rights and agreements ("terms of use," which every customer reads and signs, when opening a new account) about using your banking information? Do you know what they state?**
   Honestly, I don't know my rights and agreements, even though I have indicated in the contract with my bank that I have read them, and then signed. The reason for this is that there was a lot of writing in small fonts and I didn't have time at that point to review it all. Also even if I read it, I won't recall it later.

5. **Are you familiar with the rules of how your bank keeps, maintains and processes your cardholder data when working with it internally?**
   I am not very familiar with the rules of my bank because I never faced the situation where this information might be needed or useful to me.

6. **Are you familiar with the rules of how and to whom your credit card and cardholder data could be revealed outside of your bank? What are they about, if you know?**
   I believe that my credit card and cardholder data cannot be revealed to anyone except myself. However, I think that if there is a court order, then this information could be disclosed to government officials without my permission. But I don't know these rules either, as I didn't have to know them.

7. **Have you received, if at all, your card-statements from your bank via postal mail, e-mail or SMS?**
   I have never received any card-statements from my bank via postal mail, e-mail or SMS-notifications. I can view it on the website of my bank.

8. **If you have never received your card-statements by any of the above methods, which one of them you think is less safe for sending/receiving confidential banking information?**

   In my opinion all of these methods are really unsafe, but it also depends on what type of information is displayed on the reports. However, I think postal mail is less safe because it would go through too many services and people before it gets to me, contrary to electronic card-statement, which will reach me next few minutes it was sent out.

9. **Do you trust your bank?**

   Yes, I think so.

10. **Have you heard about your bank's data breach incidents?**

    No, I have never heard about any data breach incidents.

11. **If you don't know about your bank's data breach incident, what, in your opinion, may cause it and what consequences it might bring along for a bank and its customers?**

    I think what might cause it is poorly established data security. This incident can result in massive disclosure of personal information and it could lead to funds leak. As a consequence a bank would lose its reputation.

12. **Have you personally experienced any type of identity theft, like someone used your name, passport number, Social Security Number to gain access to your bank account and spend/transfer your money?**

    No, this never happened to me.

13. **But if this happened to you, what would be your actions?**

    If I was in the described situation I would be very scared and wouldn't know what to do. If it was regarding illegal usage of my credit/debit card I would first report it to the bank and seek their assistance. If the identity theft happened with my passport and

social security number I would report it to the local police and asked for their help. If they couldn't help me they would probably know where I would need to go.

Respondent D2

1. **Do you know what is defined under term "personal data"? Do you think your personal data has to be confidential? Do you consider your banking information - i.e. your credit card and cardholder data – to be a part of your "personal data"? Do you think your banking information has to be confidential as well?**

   I don't know what is defined as "personal data" under my contract with my bank, however I assume that all the data about me, my identification information and my financial activities are all collectively represent "personal data" and it must be protected, i.e. must be strictly confidential.

2. **Have you heard of any laws, regulations or standards that exist in the sphere of security of banking information – i.e. credit card and cardholder data - in Kazakhstan? Can you name any of these laws, regulations, and standards? Do you think your bank needs to be in compliance with them? Do you know of such laws/standards practice in other countries?**

   I have never heard of any Kazakhstani Laws and regulations and laws regarding the banking information security. However I assume most banks employ some sort of internal control mechanisms to ensure data security and privacy. However I don't think it is regulated by the state [Kazakhstan]. SOX, PCI DSS are some of the laws and regulations I am familiar with, but those are of the U.S.

3. **Are you familiar with your rights and agreements (which you get to read and sign, when opening a new banking account) about using your banking information? What are they?**

   I honestly do not remember a thing that was mentioned in that contract.

4. **Are you familiar with the security rules of how your bank keeps, maintains and processes your cardholder data when working with it internally?**
   No. I have no clue. I don't think they would introduce me to such rules, anyways.

5. **Are you familiar with the rules of how and to whom your cardholder data could be revealed outside of your bank? What are these rules about?**
   I am pretty sure that the bank cannot release any information to third parties unless my notarized authorization letter or power of attorney. But, I'm not familiar what are they.

6. **Have you received, if at all, your credit reports/statements from your bank via mail or e-mail?**
   I never received any statements neither by mail nor by email.

7. **Which of these two methods will most likely compromise your identity and confidential banking information?**
   Both of those methods are absolutely insecure way of communicating financial statements to customers, especially in Kazakhstan.

8. **Do you trust your bank?**
   Yes. I didn't have any reason not to.

9. **Have you heard about your bank's data breach incidents?**
   I have never heard about any security breaches at my bank.

10. **Have you personally experienced any type of identity theft involving fraudulent activity with your banking information?**
    No, I've never been a victim of any financial fraud or identity theft

Respondent D3

1. **Do you know what is defined under term "personal information"? Does it have to be confidential? Do you think your banking information (i.e. your credit card and cardholder dat.) has to be confidential?**

   Personal information is specific information that is considered a property of an individual, and should be revealed only to a limited group of people who have some relationship to the person (government, family). Personal information has to be confidential under most circumstances. Banking information, in my opinion, is the personal information that has a direct monetary value to it, as it might contain access to funds the individual owns. Banking information, therefore, has to be confidential.

2. **Have you heard of any laws, regulations or standards that exist in the sphere of security of credit card and cardholder data in Kazakhstan? Do you think your bank needs to be in compliance with them? Do you know of such laws/standards in other countries?**

   I haven't heard about such laws and regulations in Kazakhstan. However, I am sure that they do exist, but they may be not sophisticated.

   I'm not familiar with international legislation either. But I know that security is a key issue in the United States banking system, as the web sector grows rapidly and more information is shared over the internet. Unauthorized use of a credit card in United States is a criminal violation similar to physical theft (money and other physical property that carries a value), so the state law considers certain punishment for this violation.

3. **Are you familiar with the rights and agreements you signed at the bank about using your cardholder data? What are they?**

   To be honest, I haven't read the rights and agreements when I received my card and data attached to it. Nonetheless, I can compare the number of pages in the agreement I signed getting a card in Kazakhstan to the number of pages in the

agreement I signed getting a card in United States. My observation tells that latter is shorter. As for the card itself, the information on it suggests that the card is the property of the bank that issued it, and any misuse of the card is prohibited by law. They don't state the law, though. And I don't know what law prohibits it either.

4. **Are you familiar with the rules of how your bank uses and shares your cardholder data internally?**
   I didn't have a chance to get to know such information, but common sense suggests that those rules are included in the code of conduct of the bank. It should be similar to the code that any institution develops to protect their private internal information.

5. **Are you familiar with the regulations or rules of how and to whom your cardholder data could be revealed outside of your bank?**
   Outside of the bank, the cardholder data can be revealed only to the cardholder himself or to a person who is authorized by the cardholder.

6. **Have you received, if at all, your credit reports/statements from your bank via postal mail or Internet (e-mail)?**
   I have never received statements from my bank.

7. **Have you heard about your or any other bank's data breach incidents?**
   I cannot recall any incidents concerning data breach, however I can say that this kind of incidents usually happen because of human factor – this might include improper qualification or an unintentional mistake.

8. **Have you personally experienced, any type of identity theft targeting to gain access to your banking account?**
   No, never happened to me.

Respondent D4

1. **Do you know what is defined under term "personal information"? Does it have to be confidential? Do you think your banking information (i.e. your credit card and cardholder data) has to be confidential?**

   In my knowing, "personal data" is my full name, address, date and place of birth, SSN, passport number, and everything else that is related to my identity. I think it is OK if somebody knows my name and date of birth; however, the rest of personal data should be secured from people who I don't know. I consider that my banking information is a part of my "personal data". I am sure that it should be confidential. Nobody except bank and me should know about my credit card and cardholder data.

2. **Have you heard of any laws, regulations or standards that exist in the sphere of security of credit card and cardholder data in Kazakhstan? Do you think your bank needs to be in compliance with them? Do you know of such laws/standards in other countries?**

   No, I haven't heard about any laws, regulations or standards that exist in the sphere of security of banking information in Kazakhstan. Thus, I can't name any of them. However, if there are any, I think my bank needs to be in compliance with them. I am sorry, I don't know about such legislation practice in other countries, though.

   I think and I insist that such laws and regulations should exist in Kazakhstan legislation, if they don't exist yet. Individual's personal data should be protected anywhere

3. **Are you familiar with the rights and agreements you signed at the bank about using your cardholder data? What are they?**

   I am not familiar with my rights and agreements about using my banking information because I didn't read them. I assumed that bank protects my personal data fair enough.

4. **Are you familiar with the rules of how your bank uses and shares your cardholder data internally?**

   I am not familiar with the security rules of how my bank keeps, maintains and processes my cardholder data when working with it internally. I suppose they have internal policy to keep my cardholder data secured. I trust my bank.

5. **Are you familiar with the rules of how and to whom your cardholder data could be revealed outside of your bank?**

   I am not familiar with the rules of how and to whom my cardholder data could be revealed outside of my bank. I guess they might give information about my banking account to criminal or financial police in case if these agencies suspect me in something.

6. **Have you received, if at all, your credit reports/statements from your bank via Internet, postal mail or SMS notification? If so, what kind of cardholder information is included in there?**

   I haven't received my credit reports/statements from my bank via mail, e-mail or SMS. I check everything online by myself. My bank offered to send me SMS notifications if any operation happens from my card; however, I refused to have this service because I decided it doesn't worth money and I don't need it anyway. I don't think that there is any safe method among the mentioned above methods. However, SMS might be the safest if only information bank sends is what operation happened and when. The most unsafe might be mail, because it can be read by anybody till it gets to me.

7. **Have you heard about your bank's data breach incidents?**

   I haven't heard about my bank's data breach incidents. be bankrupt after most of its customers leave it.

8. **Have you personally experienced, if at all, any type of identity theft that targeted to your banking account?**

I didn't experience it. I hope I will not.

9. **What would be your actions, if you were in the described earlier situation (Q8)?**

   If my identity were thieved, I would call the police. I would inform my bank and other agencies that were using my personal data. I would have to immediately change my personal data in registrar office.

Respondent D5

1. **Do you know what is defined under term "personal data"? Do you think your personal data has to be confidential (secret)? Do you consider your banking information - i.e. your credit card and cardholder data – to be a part of your "personal data"? Do you think your banking information has to be confidential as well?**

   Personal information refers to the specific information used to identify an individual (e.g. first name, last name, SSN, address, etc.). some of the personal data should be confidential, but not all. Most of the concerns come from the misuse of the personal info. Misuse of the personal info such as credit card info, SSN, and personal id are always subject to identity theft and fraud. Therefore, they should be confidential. On the other hand, the likes of first name, last name, email, telephone number can be unrestricted, because they are easily accessible –i.e. from the social networking websites, telephone books, and cannot be misused to steal someone's identity.

2. **Have you heard of any laws, regulations or standards that exist in the sphere of security of banking information – i.e. credit card and cardholder data - in Kazakhstan? Can you name any of these laws, regulations, and standards? Do you think your bank needs to be in compliance with them? Do you know of such laws/standards practice in other countries?**

Yes, I have. For instance, a bank is allowed to cooperate with another bank in order to improve its business – i.e. in the sphere of security, service, cooperative projects, etc.

Every bank has to be in compliance with all regulations, standards, and laws of the country where it resists. Moreover, if a bank works both domestically and internationally, it should satisfy not only the domestic standards, but also international. For instance, in the U.S. it's mandatory for banks to inform its clients if serious theft or fraud issues occur within the bank.

3. **Are you familiar with your rights and agreements about using your banking information? What are they?**

   I'm not familiar with all of them, but basic ones such as bank's responsibility to provide maximum confidentiality to personal information of a client. However, I do have my own copy of agreement which can look if needed.

4. **Are you familiar with the security rules of how your bank keeps, maintains and processes your cardholder data when working with it internally?**

   No, I'm not. I think banks keep this information in secret. Banks can ensure clients that their personal data are kept secure, but they don't provide information how they keep them in that way.

5. **Are you familiar with the rules of how and to whom your cardholder data could be revealed outside of your bank?**

   No, I'm not familiar with them.

6. **Have you received, if at all, your card-statements from your bank via postal mail or e-mail?**

   No, I haven't received any bank statements via email, SMS or postal mail.

7. **Have you heard about your or any other bank's data breach incidents?**

   No, I haven't heard of such incidents.

8. **Have you personally experienced, if at all, any type of identity theft aimed to gain access to your banking account?**

   No, I haven't experienced any identity or credit card theft.

9. **Do you trust your bank?**

   Yes, I do.

Respondent D6

1. **Do you know what is defined under term "personal data"? Do you think your personal data has to be confidential (secret)? Do you consider your banking information - i.e. your credit card and cardholder data – to be a part of your "personal data"? Do you think your banking information has to be confidential as well?**

   Yes, I think it's all information that is my private. It must be confidential, of course. Banking information is also confidential, hence is personal.

2. **Have you heard of any laws, regulations or standards that exist in the sphere of security of banking information in Kazakhstan? Do you know of such legislation practice of other countries?**

   No, I haven't heard of such regulations neither in Kazakhstan, nor abroad. I think we should have something to regulate this topic, if we don't have them yet.

3. **Are you familiar with your rights and agreements about using your banking information? What are they?**

   Yes, I read them, but I don't remember all of them at the moment. I read my credit card agreement before signing it.

4. **Are you familiar with the security rules of how your bank keeps, maintains and processes your cardholder data when working with it internally? What are these rules about, if you know?**

   No, I have no idea. Never had questions per it.

5. **Are you familiar with the rules of how and to whom your cardholder data could be revealed outside of your bank? What are these rules about (in short)?**

   Authorized institutions, such as government, police, national security agency, tax department, etc. I think these rules are as simple as "*if requested, then provided*."

6. **Have you received, if at all, your credit reports/statements from your bank via mail or e-mail? If so, how do you usually request such reports, and what kind of cardholder information is included in there?**

   No, I haven't.

7. **Have you heard about your or any other bank's data breach incidents? If so, what were the cause of this incident(s) and its consequences for the bank and its customers?**

   No, I haven't. But I read about employee(s) who stole their bank's money, however they got caught.

8. **Have you personally experienced, if at all, any type of identity theft targeting your banking account?**

   No, I haven't.

9. **Did it happen to anyone you know personally?**

   No, none of the described have happened to anyone I know personally.